



Ebbw Fawr Learning Community  
Cymuned Ddysgu Ebwy Fawr

# eSafety Policy

<b>Author:</b>	<b>Senior Management Team</b>
<b>Date of issue:</b>	<b>January 2016</b>
<b>Review date:</b>	<b>January 2018</b>
<b>Reference:</b>	<b>EFLC – eSafety Policy.docx</b>

# CONTENTS

Introduction .....	1
eSafety .....	2
eSafety - Roles and Responsibilities.....	2
eSafety in the Curriculum.....	2
eSafety Skills Development for Staff .....	3
Managing the School eSafety Messages .....	3
Incident Reporting, eSafety Incident Log & Infringements .....	3
Incident Reporting.....	3
eSafety Incident Log .....	3
Misuse and Infringements (inc misuse flowchart).....	4
eSafety Flowchart .....	5
Smile and Stay Safe Poster.....	6

## Introduction

ICT in the 21<sup>st</sup> Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, **Ebbw Fawr** need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment. Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

Whilst exciting and beneficial both in and out of the context of school, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements, usually 13 years.

All details in this document should be read alongside the suite of ICT policies including:

- Email Policy
- eSafety Policy
- Internet and Web 2 (Social Media)Technologies Policy
- Password Policy
- Safe Use Of Images Policy

It is assumed that staff are familiar with each of these documents.

### eSafety - Roles and Responsibilities

As eSafety 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. The named eSafety co-ordinator in this school is *Mel Thomas* who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as Blaenau Gwent Council, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and governors are updated by the Head/ eSafety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and students, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies:

child protection, health and safety, home–school agreements, and behaviour/student discipline (including the anti-bullying) policy and PSHE

---

### eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the students on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The school has a framework for teaching internet skills in ICT/ PSHE lessons which can be found in the PSE scheme of work
- The school provides opportunities within a range of curriculum areas to teach about eSafety.
- Educating students about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the eSafety curriculum
- Students are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Students are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities.
- Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Cybermentors, Childline or CEOP report abuse button.
- Students are taught to critically evaluate materials and learn good searching skills through cross-curricular teacher models, discussions and via the ICT curriculum.

---

## **eSafety Skills Development for Staff**

- Our staff receive regular information and training on eSafety and how they can promote the 'Stay Safe' online messages in the form of CPD sessions, regular awareness bulletins and staff briefings.
- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowcharts in Incident, eSafety Incident Log and Infringements section).

---

## **Managing the School eSafety Messages**

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.
- eSafety posters will be prominently displayed.
- The key eSafety advice will be promoted widely through school displays, newsletters, class activities and so on.

---

## **Incident Reporting, eSafety Incident Log & Infringements**

---

### **Incident Reporting**

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's SIRO or eSafety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited e-mails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your SIRO.

---

### **eSafety Incident Log**

Keeping an incident log can be a good way of monitoring what is happening and identify trends or specific concerns.

The incident log is created automatically via the eSafety software. Currently Impero is used in school. This log is stored on the central file server and any eSafety incidents are automatically emailed to the student's form tutor so that they can be dealt with.

Dealing with issues of eSafety breach is an important role in the education of all students. We intend to educate them to become eSafe rather than banning any activity that might have an eSafety risk attached.

Any incident that may occur outside of those logged automatically, these would be very rare indeed, should be logged on a separate form kept by the ICT network managers; as below

Date & Time	Student / Staff Name	Male or Female	Room and Device number	Details of incident and evidence	Action taken and outcome

---

## Misuse and Infringements (inc misuse flowchart)

### Complaints

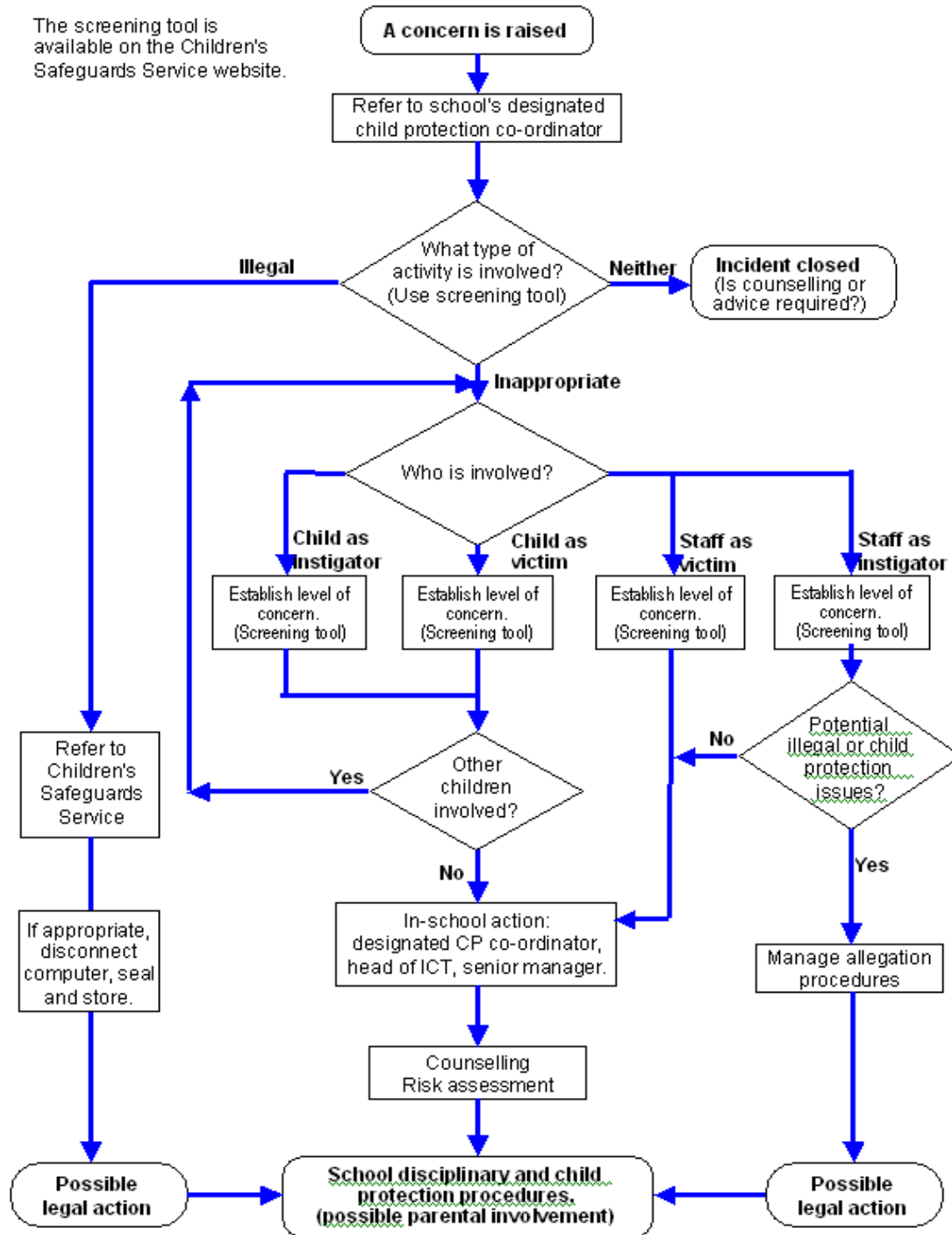
Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator or Headteacher. Incidents should be logged and the flowchart below should be followed.

### Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator and depending on the seriousness of the offence investigation by the Headteacher/ Governors with immediate suspension, possibly leading to dismissal and involvement of police for very serious offences. (see flowchart below)

# eSafety Flowchart

The screening tool is available on the Children's Safeguards Service website.



## Smile and Stay Safe Poster

eSafety guidelines will be displayed throughout school, this is the minimum standard



**S**taying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

**M**eeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you

**I**nformation online can be untrue, biased or just inaccurate. Someone online may not be telling the truth about who they are - they may not be a 'friend'

**L**et a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online

**E-mail**s, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply