The Federated Schools of the Upper Afan Valley

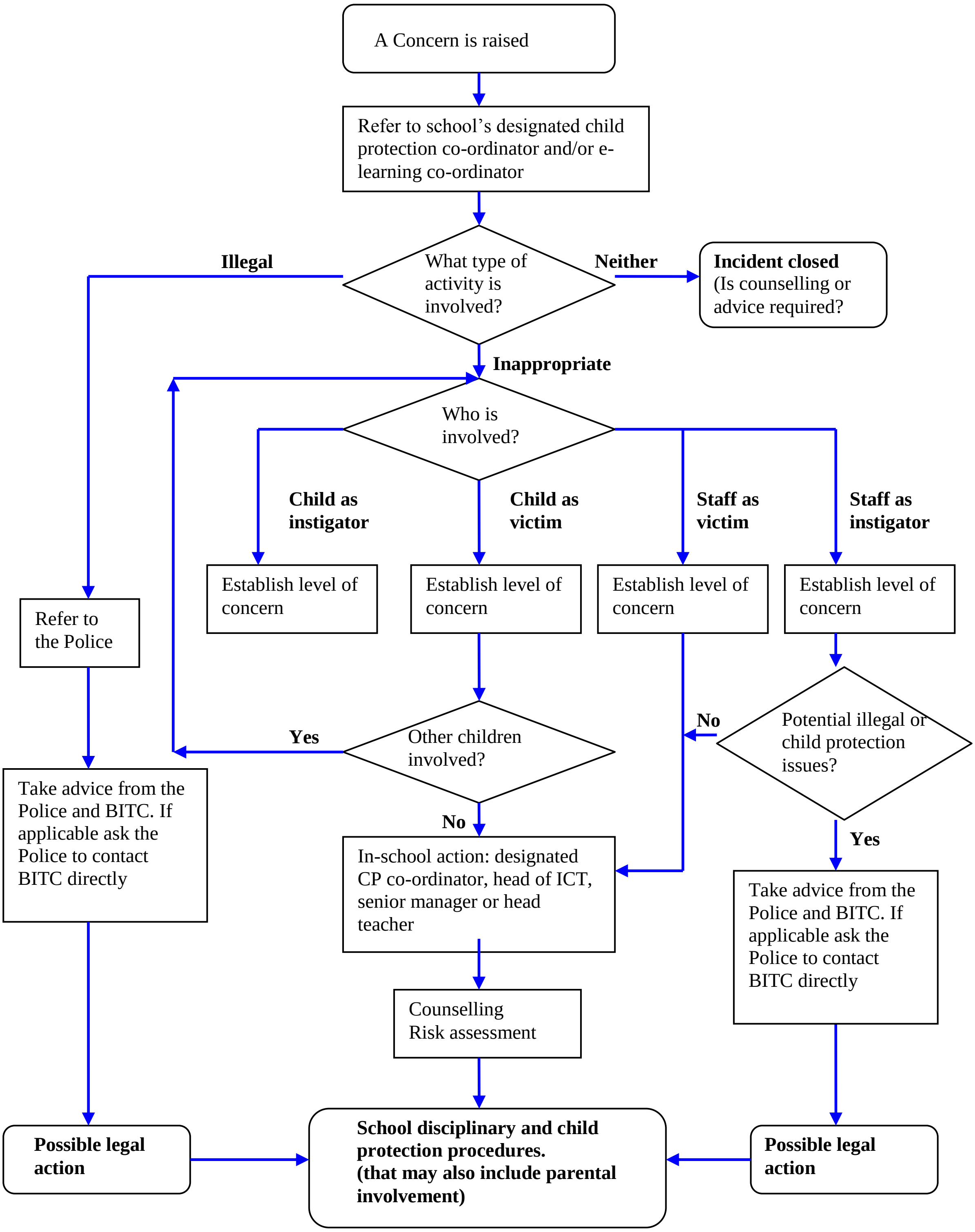
E-Safety Policy

Policy Adopted:	3rd February 2014
Additional Comments:	
Signed: M. Goodridge.	*(Chair of Governors)*

Responsibility

E-Safety depends on staff, schools, governors, advisers, parents and - where appropriate - the pupils themselves taking responsibility. Staff have a particular responsibility to supervise use, plan access and set good examples. The balance between educating pupils to take a responsible approach and the use of regulation must be judged carefully. This may be an issue that pupils could discuss and consider through Councils.

Response to an Incident of Concern



A Concern is raised
Refer to school's designated child protection co-ordinator and/or e-learning co-ordinator
What type of activity is involved?
Illegal
Neither
Incident closed
(Is counselling or advice required?
Inappropriate
Who is involved?
Child as instigator
Child as victim
Staff as victim
Staff as instigator
Establish level of concern
Establish level of concern
Establish level of concern
Establish level of concern
Refer to the Police
Other children involved?
Yes
No
Potential illegal or child protection issues?
No
Yes
Take advice from the Police and BITC. If applicable ask the Police to contact BITC directly
In-school action: designated CP co-ordinator, head of ICT, senior manager or head teacher
Take advice from the Police and BITC. If applicable ask the Police to contact BITC directly
Counselling
Risk assessment
Possible legal action
School disciplinary and child protection procedures.
(that may also include parental involvement)
Possible legal action

Who will write and review the policy?

This e-safety policy has been written by L . Lewis and will be reviewed on an annual basis.

Created: 02-05-2014

For the purpose of this document Core hours are defined as (8.30am-11.00am, 11.20am-13.20pm and 14.00pm-15.00pm)

Teaching and learning

Why is Internet use important?

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet use benefit education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the Lifelong Learning Network Wales which connects all schools in NPT;
- educational and cultural exchanges between pupils world-wide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the Local Authority and the Welsh Assembly Government;
- access to learning wherever and whenever convenient.

How can Internet use enhance learning?

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be given guidance on what Internet use is acceptable and what is not and given clear objectives for what is not.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

How will pupils learn how to evaluate Internet content?

- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- The evaluation of on-line materials is a part of every subject

Managing Information Systems

How will information systems security be maintained?

Local Area Network security issues include:

- Users must act reasonably – e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use. For Neath Port Talbot staff, flouting electronic use policy is regarded as a matter for disciplinary proceedings, that could ultimately lead to dismissal.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be pro-actively managed.

Wide Area Network (WAN) security issues include:

- All Internet connections must be arranged via the Neath Port Talbot County Network to provide an appropriate level of security and safety.
- Decisions on WAN security are made on a partnership basis between the individual school and NPTCBC. Where external access is provided to school-based systems, schools must ensure that systems are updated to avoid comprising network security.
- The security of the school information systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with NPTCBC.
- The school will work closely with NPTCBC to ensure the safety and integrity of any wireless system used or installed in school.
- School or NPTCBC data should not be stored on personal devices.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Portable media may not used without specific permission followed by a virus check.
- Unapproved system utilities and executable files will not be allowed in pupils' or staffs' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.
- The ICT co-ordinator / network manager will review system capacity regularly.

How will e-mail be managed?

- Pupils may only use approved e-mail accounts.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- The forwarding of chain letters is not permitted.
- Access in school to external personal e-mail accounts may be blocked.
- Excessive social e-mail use can interfere with learning and may be restricted. Social e-mail should not be sent during Core hours.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

How will published content be managed?

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published.
- E-mail addresses should be published carefully, to avoid spam harvesting.

- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

Can pupil's images or work be published?

- Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

- Written permission from parents or carers will be obtained before images of pupils are electronically published.

- Work can only be published with the permission of the pupil and parents.

Please see the Becta site, "use of photographic images of children".

How will social networking and personal publishing be managed?

- Social Network sites and newsgroups will be filtered unless a specific use is approved. (Schools have a responsibility to report any additional sites that they need filtered/blocked)

- Newsgroups will be blocked unless a specific use is approved.

- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.

- Teachers' official blogs or wikis should be password protected and run from the school website. Teachers should be advised not to run social network spaces for student use on a personal basis.

- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. House number, street name or school.

- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.

- Students should be advised not to publish specific and detailed private thoughts.

- Schools should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

How will filtering be managed?

- The school will work with NPTCBC, taking into account Becta guidelines, to ensure that systems to protect pupils are reviewed and improved.

- If staff or pupils discover unsuitable sites, the URL must be reported to the e-safety Coordinator and forwarded to Neath Port Talbot County Council IT service desk immediately.

- All Internet access in the school will be logged

- Internet use will be randomly monitored to ensure compliance with school policy.

- Larger schools, generally secondary, will manage the configuration of their filtering. This task requires both educational and technical experience.

- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

- Any material that the school believes is illegal must be reported to appropriate agencies.

- The school's filtering strategy will be designed by educators to suit the age and curriculum requirements of the pupils, advised by engineers.

How can emerging technologies be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

How should personal data be protected?

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

How will Internet access be authorised?

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.

- All staff must read and sign the 'Staff Acceptable Use Policy' before using any school ICT resource.

- Students must apply for Internet access individually by agreeing to comply with the e-Safety Rules.

- Parents will be asked to sign and return a consent form for pupil access within their Planners.

How will risks be assessed?

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor NPTCBC can accept liability for the material accessed, or any consequences resulting from Internet use.

- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

How will e-safety complaints be handled?
Possible statements:

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Discussions will be held with the local Community Police Officer to establish procedures for handling potentially illegal issues.
- Sanctions within the school discipline policy include:
    - interview/counselling by the head of year;
    - informing parents or carers;
    - removal of Internet or computer access for a period.

How is the Internet used across the community?

- The school will liaise with local organisations to establish a common approach to e-safety.
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

Communications Policy
How will the policy be introduced to pupils?

- E-Safety rules will be posted in rooms with Internet access.
- Pupils will be informed that network and Internet use will be monitored.
- An e-safety programme will be introduced to raise the awareness and importance of safe and responsible internet use.
- Guidelines in responsible and safe use should precede Internet access.
- An e-safety module will be included in the ICT programmes covering both school and home use.

How will the policy be discussed with staff?

- All staff will be given the School e-Safety Policy and its application and importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school e-safety Policy will be provided as required.

How will parents' support be enlisted?

- Parents' attention will be drawn to the school's e-Safety Policy in the Pupil Planner, newsletters and on the school website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.