Ysgol Greenfield School

"Opening doors to the future"

CYNGOR BWRDEISTREF SIROL MERTHYR TUDFIL

MERTHYR TYDFIL COUNTY BOROUGH COUNCIL

GREENFIELD SCHOOL

E SAFETY POLICY

Wayne Murphy, Head Teacher.
Rachel Faulkner, Deputy Head - Standards
Carol Conway, Deputy Head - Wellbeing
Gwyn Daniels - Assistant Head

' Opening Doors To The Future '

' Agor drysau i'r dyfodol'

Original Completion Date	**Author**
October 2015	Kira John, Teacher

MONOTORING THE POLICY

This policy will be reviewed bi-annually unless change of circumstances or legislation requires it to be amended earlier.

Signed: …….. Date: ……..

Head teacher

Signed: …….. Date: ……..

Chair of Governors

Review Date **Author**

Our Vision

'To open doors to the future'

Our Mission Statement

That children, staff, parents, carers and all stakeholders work actively in partnership to enable all pupils to realise and reach their full potential.

Aims

- For pupils to operate as independent learners and thinkers
- To inspire a love for learning
- To provide a relevant curriculum for all
- For pupils to value themselves
- To foster a sense of belonging to a community

Our Values

- We create
- We respect each other
- We try our best
- We are a team
- We learn from mistakes
- We celebrate each other's success
- We are polite and considerate
- We produce magic moments

We want every child to be safe and happy in our school. We believe that the key to this is for us all to have self-respect, respect for others and respect for property.

Everyone has the right to:

- Feel safe, cared for and respected.
- Be able to learn to the best of his/her ability and to develop whatever skills he/she possesses.
- Be treated equally irrespective of gender, race, physical characteristics or any other factors.
- Learn and play without disruption.

Everyone is expected to:

- Be responsible for their own behaviour
- Respect the rights of others
- Share our values

Background / Rationale

The use of exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

The improper or usage use of technology can present challenges to children, young people, volunteers and staff.

Some of the potential risks could include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to exploitation and abused 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
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.
- Blackmail involving threats to life, dignity and violence
- Poor or inappropriate supervision of Internet access leading to the viewing of harmful or inappropriate images
- Risk of sexual exploitation

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The 2011 Education Act increased these powers with regards to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published behaviour policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that takes place out of school.

Roles and Responsibilities

Head teacher and Senior Leaders:

- The Head teacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the *E-Safety Co-ordinators (see below)*.
- The head teacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinators and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant

- The head teacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the E-Safety Co-ordinators.
- The head teacher and another member of the Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents and online safety incident included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures)

E-Safety Coordinators:

- leads the e-safety committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- provides training and advice for staff including how to be alert to the potential misuse of digital media and take responsibility for reporting it appropriately
- liaises with the Local Authority
- liaises with ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of e-Safety matters and of the current school e-Safety policy and practices
- They have read, understood and signed the Staff Acceptable Use Policy
- They report any suspected misuse or problem to the Head teacher / Senior Leadership Team, E-Safety Coordinators for investigation / action
- All digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- E-Safety issues are embedded in all aspects of the curriculum and other activities
- Students / pupils understand and follow the e-Safety and acceptable use agreements / policies
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Safeguarding Designated Person

The Safeguarding Designated Person *(C. Conway)* is trained in e-Safety issues and is aware of the potential for serious safeguarding issues that could arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

E-Safety Group

Members of the e-Safety Group (W. Murphy, C. Conway, G. Daniels) will assist the *e-Safety Coordinators* (K. John &A. Connor*)* with:

- The production / review / monitoring of the school e-Safety policy / documents
- The production / review / monitoring of the school filtering policy (if possible and if the school chooses to have one) and requests for filtering changes
- Mapping and reviewing the e-Safety curricular provision – ensuring relevance, breadth and progression
- Monitoring network / internet / incident logs where possible
- Consulting stakeholders – including parents / carers and the pupils about the e-Safety provision

Students / pupils:

- Are responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Agreement
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying
- Should understand the importance of adopting good e-Safety practice when using digital technologies out of school and realise that the schools e-Safety Policy covers their actions out of school, if related to their membership of the school

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. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-Safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-Safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website and on-line student / pupil records
- Their children's personal devices in the school (where this is allowed)

Visiting Adults and Pupils

- Users who access school ICT systems / website / Hwb via login as part of the Extended School provision will be expected to sign an AUP before being provided with access to school systems.

Policy Statements

Education – young people

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-Safety is therefore an essential part of the school's e-Safety provision. Children and young people need the help and support of the school to recognise and avoid e-Safety risks and build their resilience.

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

- A planned e-Safety curriculum should be provided as part of ICT / PSE / or other lessons and should be regularly revisited
- Key e-Safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – parents / carers

Many parents and carers have only a limited understanding of e-Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

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

Cyberbullying

Cyber bullying has become an increasing concern for schools, parents and children alike. Cyber bullying has traditionally been defined as harassment and victimisation using interactive technology. It is important that we understand the complex nature of cyber bullying to be able to prevent incidents and respond effectively to incidents when they arise. For example, one comment made online becomes bullying when it is repeatedly forwarded or commented on by others, which in turn is seen by multiple people over a sustained period of time. It can often be difficult to gain closure when subject to a cyber bullying incident when the comment or photo can resurface at any time.

Cyber bullying differs from traditional forms of bullying and can have a significant detrimental impact upon individuals who are targeted by such behaviour. The 24/7 nature of cyber bullying can make it difficult for a target to escape the attacks directed at them. In some cases an individual may not know they are being bullied if they have not seen the content posted about them, but it is important to understand that the intentions of the perpetrator is still to bully the individual in question by posting humiliating and hurtful content.

We promote the positive use of Interactive Technology and Social Media, where pupils are provided with opportunities to discover the benefits social media has to their learning and social development. We understand that it can sometimes be easy to forget that we are talking to real people with real emotions when using social media; as such we encourage and promote responsible use and respectful communications with others online.

All incidents of inappropriate use of social media are taken seriously and we encourage all members of the school community to report any incidents of inappropriate use of social media and interactive technology.

Inappropriate use of social media includes, but not restricted too:

- harassment and intimidation of others
- sending hateful messages
- posting inappropriate and unwanted pictures online
- creating content which has the potential to hurt, embarrass and humiliate others
- Sexting
- Online exploitation including sexual abuse

We respond to inappropriate use and bullying online in accordance with the procedures and guidance outlined in our anti-bullying and behaviour policy. Support is provided to all parties involved in incidents of bullying online and parents will be notified following a report of bullying online. Where appropriate we will contact external agencies to obtain further advice, information and provide additional support to individuals if necessary. Restorative approaches will be implemented to resolve any issues of inappropriate use of social media. We understand that in some circumstances there will be a requirement to involve the police. We will liaise with our Police School Liaison Officer for advice on the appropriate route and action to take in these circumstances.

Education & Training – Staff / Volunteers

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

- A planned programme of formal e-Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-Safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-Safety as a training need within the performance management process.
- All new staff should receive e-Safety training as part of their induction programme, ensuring that they fully understand the school e-Safety policy and Acceptable Use Agreements.
- The e-Safety Coordinator will receive regular updates through attendance at external training events (e.g. from Consortium / SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This e-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The e-Safety Coordinators will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in e-Safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in technology / e-Safety / health and safety / safeguarding . This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association/ or other relevant organisation (e.g.. SWGfL).
- Participation in school training / information sessions for staff or parents

Technical- Infrastructure/equipment, filtering and monitoring

Technical
The control, management and monitoring of infrastructure and equipment (internet filtering system and network resources; data; share; services and software) play a key role in e-safety. This section of the document outlines schools and individuals responsibilities when setting up, connecting and using ICT equipment.

Context
The school is connected to a shared network. Clients, servers and users connecting to the network are administrated by the MTCBC ICT department. The school has access to a managed wireless and wired network, a filtered internet connection and firewall protection. These services are configured with policies and controls to prevent misuse, malicious attack and to ensure the protection and safety of our data, staff and learner.
The managed service is subject to condition of use, as outlined in the MTCBC Broadband terms and conditions documents and the schools responsibilities section of the ICT Support SLA.
It is the schools responsibility to ensure that the users of ICT systems and equipment are aware of, have access to and have signed the appropriate Acceptable Use Policies.

Connections to the school network:

- Equipment connected to the Shared Schools Network should be owned by the school and in line with the limitations set out in the Schools ICT Support SLA
- Antivirus: In line with the Schools Broadband Terms and Conditions, it is the schools responsibility to ensure workstations and other devices are protected by the up to date virus software.

- Appropriate security measures are in place to protect the servers, networking equipment, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These measures should not be circumvented or attempts made to do so.

Internet Filtering

- The school uses and supports managed filtering service provided by MTCBC ICT Department.
- Any filtering issues should be reported immediately to the MTCBC ICT Department Helpdesk.
- In accordance with the MTCBC internet acceptable use policy, school ICT technical or MTCBC ICT staff may monitor and record the activity of users on the school ICT systems. Users are made aware of this in the Acceptable Use Policy.

Access, Controls and Restrictions

- Users will be made responsible for the security of their username and password and 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.
- All users will have clearly defined access rights to schools ICT systems.
- Servers, wireless systems and cabling must be securely located and with physical access restricted.
- Regular reviews and audits of the safety and security of school ICT systems should be undertaken.
- Schools should limit the potential for data loss, data security incidents and the spread of malicious software by controlling the use of removable media.
- Removable media should not be used to transfer data between the administrative and curriculum networks.
- Users may only be granted access to the network/system/software/data resources for which they have a requirement to use.
- An agreed policy is in place for the provision for temporary access of 'guest' (e.g. trainee teachers, visitors) onto the school system.

Information Security

- MTCBC/ School owned portable ICT equipment should be used in accordance with the schools remote working policy.
- Personal data about individual staff and learners cannot be sent over the internet (e-mail, attachment or other upload) or taken off the school site unless safely encrypted or otherwise secured.
- Information security incidents should be logged with the information security officer at the earliest opportunity.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils 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.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the student / pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults			Students / Pupils				
Communication Technologies	Allowed	Allowed at certain times	Not Allowed	Allowed with supervision **Post 16** Department	Allowed	Allowed at certain times	Allowed with staff permission And supervision	Not allowed
Mobile phones may be brought to school	x			x				x
Use of mobile phones in lessons								x
Use of mobile phones in social time		x		x				x
Taking photos on mobile phones / cameras								x
Use of other mobile devices e.g. tablets, gaming devices							x	
Use of personal email addresses in school, or on school network			x					x
Use of school email for personal emails			x					x
Use of messaging apps		x		x				x
Use of social media		x		x		x		
Use of blogs		x		x		x		

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school or on school systems (e.g. by remote access) .Pupils names should not be used in emails.
- Users must immediately report to the nominated person – in accordance with the school policy - the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, chat etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils may be provided with individual school email addresses for educational use.
- Pupils should be taught about e-Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out by the General Teaching Council Wales (GTCW) but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. All staff working at any educational establishment are expected to demonstrate a professional approach and respect for pupils and their families and for colleagues and the learning setting.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

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

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and e-Safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain	Acceptable for nominated	Unacceptable	Unacceptable and
Users shall not visit Internet sites,	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X

make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.**					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)	X					
On-line gaming (non educational) supervised		X				
On-line gambling				X		
On-line shopping / commerce		X				
File sharing		X				
Use of social media		X				
Use of messaging apps		X				
Use of video broadcasting e.g. Youtube		X				

Responding to incidents of misuse

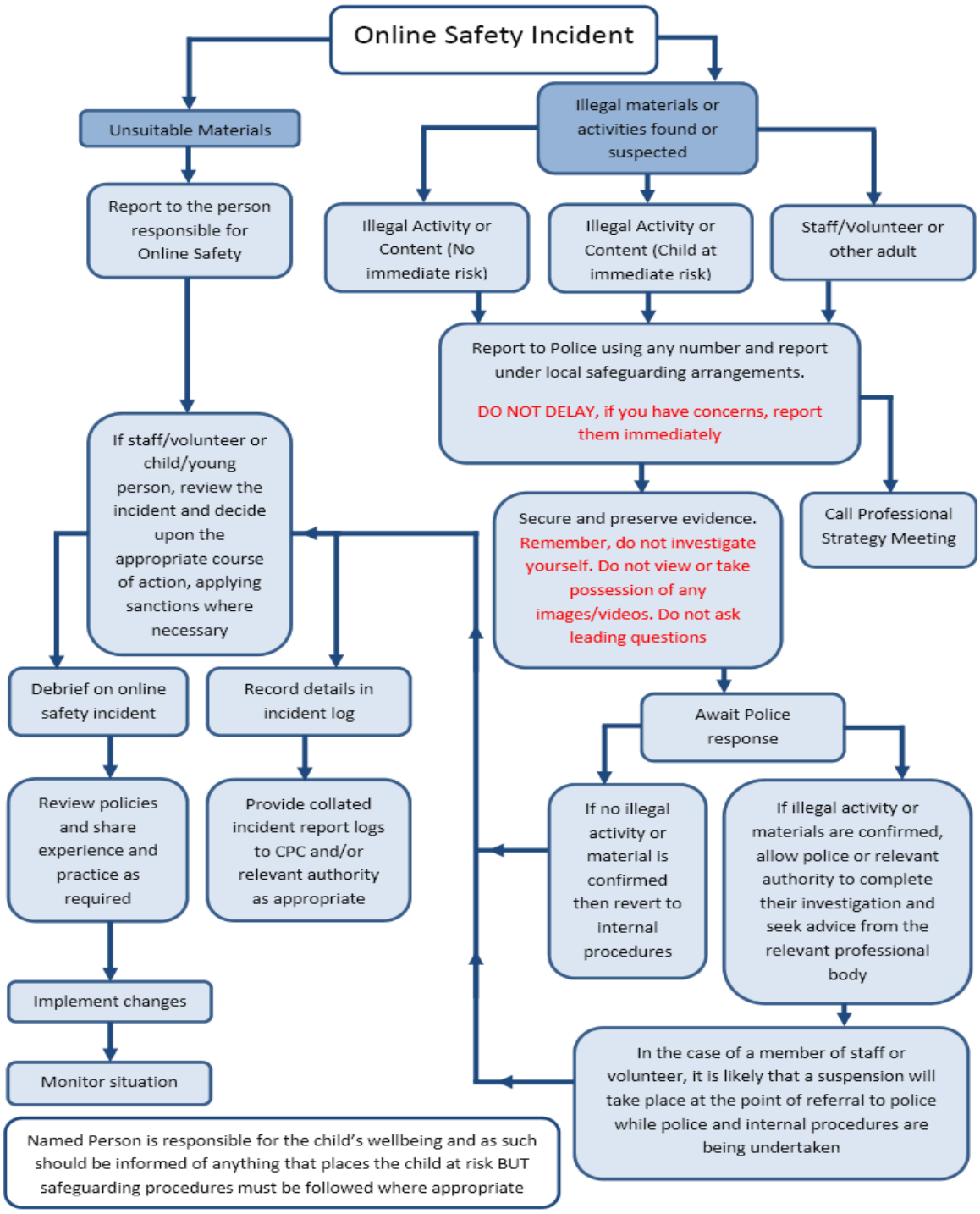
It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or

irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Please follow the flow chart on the next page:



Other Incidents

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

- 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
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

School Actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students / Pupils **Actions**

Incidents:	Refer to class teacher	Refer to Head of Department	Refer to Head teacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	X						X		
Unauthorised use of mobile phone / digital camera / other mobile device	X						X		
Unauthorised use of social media / messaging apps / personal email	X						X		

Unauthorised downloading or uploading of files	X						X		
Allowing others to access school network by sharing username and passwords	X						X		
Attempting to access or accessing the school network, using another student's / pupil's account	X						X		
Attempting to access or accessing the school network, using the account of a member of staff	X						X		
Corrupting or destroying the data of other users	X	X					X		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X					X	X	
Continued infringements of the above, following previous warnings or sanctions	X	X	X			X	X	X	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X			X	X	X	
Using proxy sites or other means to subvert the school's 's filtering system	X	X	X			X	X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X						
Deliberately accessing or trying to access offensive or pornographic material	X	X	X			X	X	X	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X				X	X	

Staff **Actions**

Incidents:	Refer to SMT	Refer to Head teacher	Refer to Local Authority / HR/ICT Department	Refer to Police	Refer to Technical Support Staff for action re filtering	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email	X	X				X		
Unauthorised downloading or uploading of files	X	X						
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X						
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X						
Deliberate actions to breach data protection or network security rules	X	X				X		

Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X				X		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X				X		
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X				X		
Actions which could compromise the staff member's professional standing	X	X						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X				X		
Using proxy sites or other means to subvert the school's 's filtering system	X	X						
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X					
Deliberately accessing or trying to access offensive or pornographic material	X	X	X					
Breaching copyright or licensing regulations	X	X						
Continued infringements of the above, following previous warnings or sanctions	X	X	X			X		