

Porthcawl Comprehensive School



E-Safety Policy

CONTENTS

	Page
Policy Statement	3
Roles	4-5
Technical information	5-6
BYOD	6-7
Images	7
Data Protection	8
Guidelines	9-10
Social Media	10-11
Unsuitable activities	11-12
Flowchart	13
Other incidents	14
School Actions	15-17
BCBC Six Simple Rules	18
List of appendices	19
Pupil/student AUA	20-22
Staff/volunteer AUA	23-25
Parent/carer AUA	26-27
Technical Security Policy	28-32
Personal Data Handling Policy	33-43
BCBC Information Transmission Guidance	44
BCBC Information Disposal Guidance	45
BYOD Policy	46
Social Media Policy	47-52
Application for Social Media Account	53
E-Safety group Terms of Reference	54-55
Record of reviewing sites (for internet misuse)	56
Reporting Log	57
Summary of Legislation	58-61
Links to other organisations and documents	62-64
Glossary of terms	65

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

This policy should be read in conjunction with the school's Anti-Bullying policy, Safeguarding Policy and Behaviour Policy, as well as with reference to the documents attached in the appendix.

Policy Statement

Whilst regulation and technical solutions are very important, their use must be balanced by educating students / pupils to take a responsible approach. The education of students / 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 / Computing / PSE 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
- Students / 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.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students / pupils should be helped to understand the need for the student / 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 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.
- Where students / 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 (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Senior ICT Technician, in consultation with senior 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/carers 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, website, Twitter
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications

Eg: <https://hwb.wales.gov.uk/>
www.saferinternet.org.uk/
<http://www.childnet.com/parents-and-carers>

(See appendix for further links / resources)

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 (eg 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.
- This e-Safety policy and its updates will be presented to and discussed by the Governing Body in Governing Body meetings.
- The e-Safety Coordinator will provide advice / guidance / training to individuals as required. E.g. Student teachers, long term cover staff

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 (eg SWGfL).
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their e-Safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling will be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the Senior ICT Technician Luke Rowberry who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password *and will be required to change their password every 90 days.*
- The “master / administrator” passwords for the school ICT system, used by the Senior ICT Technician must also be available to the Headteacher or other nominated senior leader and kept in the school safe.
- The Senior ICT Technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider.
- The school has provided differentiated user-level filtering (allowing different filtering levels for different groups of users – staff / pupils / students)
- Where possible, school technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

- Agreed procedure is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.
- Acceptable Usage Agreements are in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- Acceptable Usage Agreements are in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the school allowing staff and older pupils to bring in their own technologies in order to provide a greater freedom of choice and usability.

A device may be a privately owned smartphone (staff only), tablet, notebook / laptop or other new technology that has the capability of utilising the school’s wireless network. The device then has access to the wider internet including the school’s Hwb+ learning platform and other cloud based services such as email and data storage.

The students, staff and wider school community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device they use is user or school owned. This understanding then underpins further conventions around acceptable use of both the devices and of the wider network.

Potential Benefits of BYOD

Research is highlighting the widespread uptake of portable, wireless enabled electronic devices amongst adults and children of all ages. This technology exists as part of their everyday digital world and by allowing them to use these devices freely in school, the school is bringing that familiar digital life into the school classroom. Learners will no longer have to ‘power down’ when they walk through the doors of the school and can engage with and own their learning more effectively. BYOD has the potential to maximise the huge investments that have been made in the schools’ infrastructure and allows for greater opportunity to engage with learning technologies.

Considerations

The BYOD policy sits alongside a range of policies including but not limited to the Safeguarding Policy, Bullying Policy, Acceptable Usage Policy, policies around theft or malicious damage and the Behaviour Policy.

Practical rules include:

- Screens must be visible at all times i.e. face up on the desk
- Teachers and/or students must be allowed to view any student device
- Photographs and videos cannot be taken without the authorisation of the teacher
- Breaches of the trust being given to the students will be dealt with according to sanctions identified in the Acceptable Usage Agreement.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying 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 students / 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 eg 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 *students / 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 students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs unless parental/carer permission has been received.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website/Twitter accounts.
- Student's / 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.e.g. S2S, CTF

The school will 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". (see Privacy Notice section in the appendix)
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- It has clear and understood 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 arrangements for the deletion and disposal of data
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties

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.
- Only 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 (below) once it has been transferred or its use is complete

Communications Guidelines

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:

Communication Technologies	Staff & other adults				Students / Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X				X			
Use of mobile phones in lessons		X				X	X	
Use of mobile phones in social time	X				X			
Taking photos on mobile phones / cameras		X						X
Use of other mobile devices eg tablets, gaming devices	X					X	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
Use of social media			X				X	
Use of blogs			X					X

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

- The official school email service may be regarded as generally safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students / pupils should therefore use only the school email service to communicate with others when in school, or on

school systems (eg by remote access). **Where sensitive information is being transferred staff MUST use their Bridgend email.**

- 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 students / pupils or parents / carers (email, chat, VLE 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 accounts must not be used for these communications.
- Students / pupils will be provided with individual school email addresses for educational use.
- Students / 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

The school has a clear and up to date Social Media Policy. Expectations for teachers' professional conduct are set out by the Education Workforce Council (EWC) 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.

The school has a duty of care to provide a safe learning environment for pupils and staff. The school and Bridgend Local Authority 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. All staff working at Porthcawl Comprehensive School 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 ICT Technician, e-Safety Coordinator and the e-Safety committee to ensure compliance with the Social Media Policy, Data Protection Policy and Acceptable Usage Agreements.

Unsuitable / inappropriate activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities eg 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 times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	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	

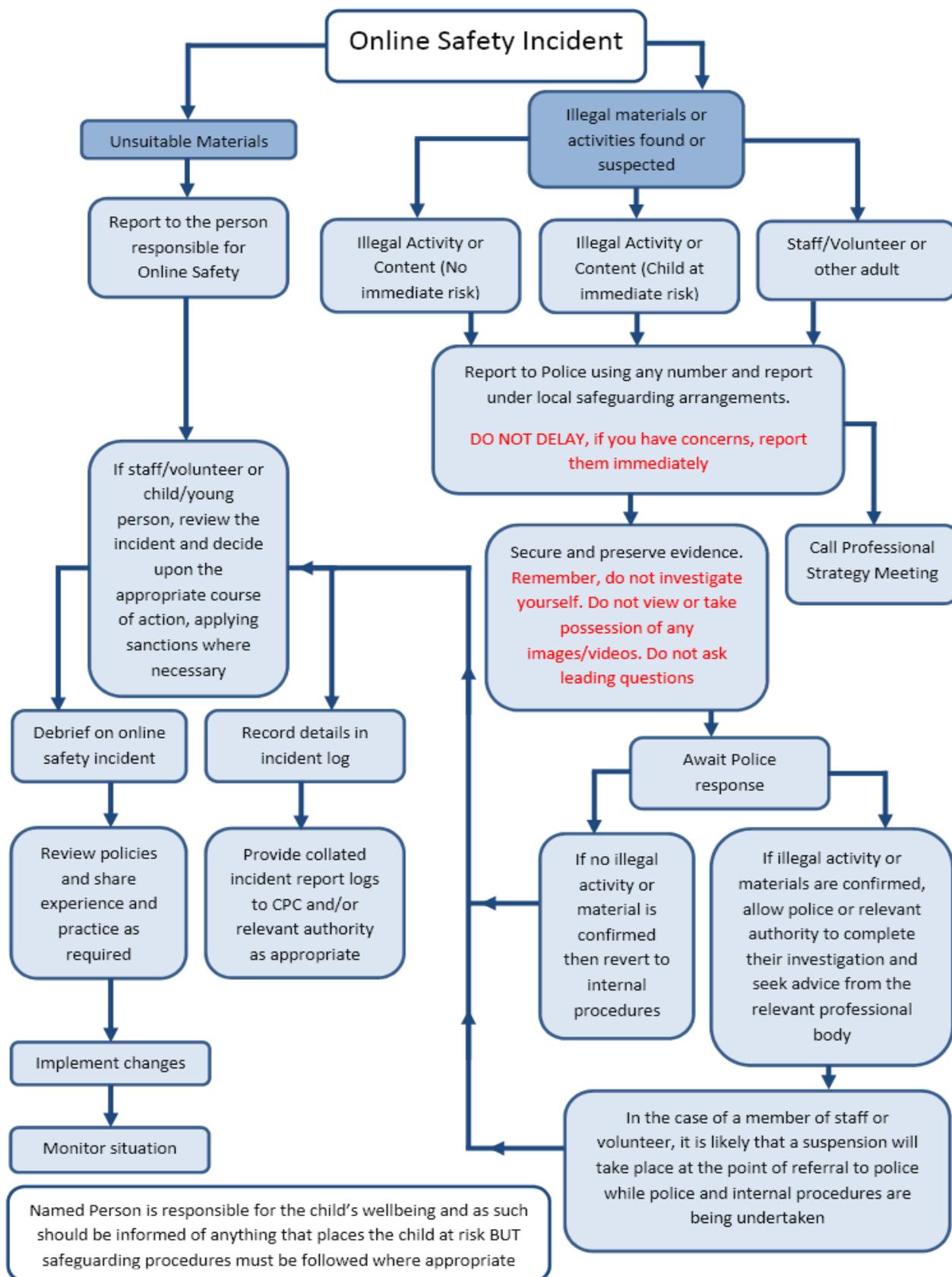
or relate to:	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
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 (eg 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)					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 eg Youtube				X		

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart below for responding to online safety incidents and report immediately to the Headteacher or Designated Child Protection teacher.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

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

- Have more than one senior member of staff involved in this process.(A.Slade and J. Sloggett) 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 may include

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher	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 eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal			X		X	X	X		X
Unauthorised use of non-educational sites during lessons	X	X				X			X
Unauthorised use of mobile phone / digital camera / other mobile device	X	X			X	X	X	X	
Unauthorised use of social media / messaging apps / personal email	X	X				X	X	X	
Unauthorised downloading or uploading of files		X			X	X	X		X
Allowing others to access school network by sharing username and passwords	X				X	X	X	X	
Attempting to access or accessing the school network, using another student's / pupil's account		X			X	X	X	X	
Attempting to access or accessing the school network, using the account of a member of staff			X		X	X	X	X	X
Corrupting or destroying the data of other users		X			X	X	X		X
Sending an email, text or message that is		X				X	X	X	X

regarded as offensive, harassment or of a bullying nature									
Continued infringements of the above, following previous warnings or sanctions			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
Using proxy sites or other means to subvert the school's filtering system			X		X	X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident		X			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

Staff

Actions may include

Incidents:	Refer to line manager	Refer to Head teacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal		X	X	X				X
Inappropriate personal use of the internet / social media / personal email	X					X		
Unauthorised downloading or uploading of files	X				X	X		
Allowing others to access school network by sharing username and		X			X			X

passwords or attempting to access or accessing the school network, using another person's account								
Careless use of personal data eg holding or transferring data in an insecure manner		X			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		
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		
Using proxy sites or other means to subvert the school's filtering system		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
Breaching copyright or licensing regulations		X				X		
Continued infringements of the above, following previous warnings or sanctions		X	X				X	

BCBC Six Simple Rules

ICT is “Information and Communications Technology”. This includes computers, software and mobile telephones.

These rules provide a summary of the detailed ICT policies available on the Intranet –everybody must remember and abide by **these** rules. These rules form part of the council’s discipline policy.

If you are unsure about how a rule applies, first check the detailed policies on the Intranet. If you are still unsure, contact the ICT service desk for advice.

Remember – we have these rules to keep us **S E C U R E**

1. **S for Security:** You must not attempt to circumvent our security and protection measures, or encourage or allow others to do so.
2. **E for Email Use:** You must only use your BCBC-provided email addresses (e.g. someone@bridgend.gov.uk) for business purposes.
3. **C for Council Purposes:** You must only use ICT provided by BCBC for BCBC’s purposes. There are a few exceptions to this given in this policy.
4. **U, because it’s YOUR password:** You must not give your password to anyone, including IT staff, nor allow others to find it out. Accounts not in a personal name (e.g. counter accounts) may only be shared with staff in that job function.
5. **R for Report it:** You must report any suspected breach of these rules, or suspicions about security breaches to the ICT Service Desk.
6. **E for Ethical:** You must use equipment and data in an ethical, appropriate and legal manner. This includes, for example, copyright rules and data protection legislation.

During breaks, i.e. when you are marked as “out” on your flexi sheet, you may use your BCBC-provided ICT equipment for certain personal uses. These are:

- Browsing the internet.
- Using external email accounts e.g. Hotmail.
- Playing music on CDs, if your manager permits it. Originals, not copies – you also must not copy – “rip” - them onto your machine or the network.
- Work-related social organising e.g. arranging social evenings for staff. Emails for these **may** be sent on the internal system. Note that emailing jokes, gossip etc. is **not** permitted.

Please remember that all ICT use is monitored, including that in breaks; only the **C for Council Purposes** rule is partially relaxed during breaks.

Authorised USB devices such as USB storage (memory sticks), digital cameras, and scanners are permitted for use.

An authorised USB storage device is one that has been purchased via the ICT Service Unit and has been fully encrypted.

Appendices

Section A - Acceptable Use Agreements

- A1 Student / Pupil Acceptable Use Agreement
- A2 Staff and Volunteers Acceptable Use Agreement
- A3 Parents / Carers Acceptable Use Agreement

Section B – Specific Policies

- B1 School Technical Security Policy
- B2 School Personal Data Policy
- B3 School Bring Your Own Devices (BYOD) Policy
- B4 Social Media Policy
- B5 School e-Safety Committee Terms of Reference

Section C – Support documents and links

- C1 Record of reviewing sites (for internet misuse)
- C2 School Reporting Log
- C3 Summary of Legislation
- C4 Links to other organisations and documents
- C5 Glossary of terms



Student / Pupil Acceptable Use Agreement (AUA)

School Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that students / pupils will have good access to digital technologies to enhance their learning and will, in return, expect the students / pupils to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of IT systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.

- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal device(s) in school if I have permission. I understand that, if I do use my own device(s) in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, exclusions, contact with parents/carers and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.



Porthcawl Comprehensive School

Student / Pupil Acceptable Use Agreement Form

This form relates to the student / pupil Acceptable Use Agreement, to which it is attached. Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) eg mobile phones, tablets, cameras etc
- I use my own equipment out of the school in a way that is related to me being a member of this *school* eg communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student / Pupil

Group / Class

Signed

Date

Parent / Carer Countersignature

Signed

Date

Porthcawl Comprehensive School



Staff (and Volunteer) Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers have good access to ICT to enhance their work, to enhance learning opportunities for students / pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-Safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor wherever possible my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE/Twitter) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. I am fully aware of the risks attached to using personal email addresses / mobile phones / social networking sites for such communications.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school :

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Personal and Identifiable Data Security Good Practice Guide within the School Handbook. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school :

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

Appendix A3



Parent / Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-Safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that students / pupils will have good access to digital technologies to enhance their learning and will, in return, expect the students / pupils to agree to be responsible users. A copy of the Student / Pupil Acceptable Use Agreement is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents/Carers are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above student / pupil, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-Safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including applying monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-Safety.

Signed

Date

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Students / Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website/Twitter and occasionally in the public media.

The school therefore wishes to comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people can not be identified by the use of their names.

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 students / pupils in the digital / video images.

Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents / carers to agree

Digital / Video Images Permission Form

Parent / Carers Name

Student / Pupil Name

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

Yes / No

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

Yes / No

Signed

Date



Porthcawl Comprehensive School

Technical Security Policy

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of the Network Manager Luke Rowberry.

Technical Security

Policy statements

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities:

- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.

- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff
- All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be approved by the Network Manager and Deputy Head and will be recorded by the Network Manager. These will be reviewed, **at least annually**, by the E-Safety Committee.
- Users will be made responsible for the security of their username and passwords and must not allow other users to access the systems using their log on details. All users must immediately report any suspicion or evidence that there has been a breach of security.
- The Network manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Mobile device security and management procedures are in place - see BYOD agreement.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Remote management tools are used by staff to control workstations and view users activity
- An agreed process is in place for the provision of temporary access of “guests” (e.g. trainee teachers) onto the school system.
- An agreed policy is in place and described in the E-safety policy regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. (see School Personal Data Policy for further detail)
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc
- Personal data should not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see School Personal Data Policy for further detail)

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE). Where sensitive data is in use via SIMS the school uses a more secure form of authentication e.g. two factor authentication. Such items must be stored separately from the laptop when in transit – to avoid both being lost / stolen together.

Policy Statements

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the E- Safety Committee.

- All school networks and systems will be protected by secure passwords that are regularly changed
- The “master / administrator” passwords for the school systems, used by the technical staff are available to the Headteacher / and kept in the school safe.
- All users (adults and young people) will have responsibility for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords for new users, and replacement passwords for existing users, will be allocated by the Network manager Luke Rowberry.
- Users will change their passwords at regular intervals – as described in the staff and student / pupil sections below
- Where passwords are set / changed manually requests for password changes should be authenticated by the Network Manager to ensure that the new password can only be passed to the genuine user .

Staff Passwords

- All staff users will be provided with a username and password by the Network Manager who / which will keep an up to date record of users and their usernames.
- the password should be a minimum of 7 characters long and must include three of – uppercase character, lowercase character, number, special characters
- the account should be “locked out” following five successive incorrect log-on attempts or 5 minutes of inactivity
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- should be changed at least every 42 days and be significantly different from previous passwords created by the same user. The last nine passwords cannot be re-used.

Student / Pupil Passwords

- All users will be provided with a username and password by the Network manager who / which will keep an up to date record of users and their usernames.
- Users will be required to change their password every 42 days.
- Pupils will be taught the importance of password security

Training / Awareness

Members of staff will be made aware of the school’s password policy:

- at induction
- through the school’s E- safety policy and password security policy
- through the Acceptable Use Agreement

Pupils / students will be made aware of the school’s password policy:

- in lessons through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The Network Manager will ensure that full records are kept of:

-

- User Ids and requests for password changes
- User log-ins
- Security incidents related to this policy

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the Network Manager. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must be reported to a second responsible person, in this case the ICT Technician.

All users have a responsibility to report immediately to the Network Manager any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- The school has provided enhanced / differentiated user-level filtering through the use of the Barracuda Fire Wall filtering programme. (allowing different filtering levels for different groups of users – staff / pupils / students etc.)
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher
- Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems

- Any filtering issues should be reported immediately to the filtering provider.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and E-safety Co-ordinator. (If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E- Safety Committee).

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, Inset.

Parents/carers will be informed of the school's filtering policy through the Acceptable Use Agreement and through online safety awareness sessions / newsletter etc.

Changes to the Filtering System

Users may request changes to the filtering (eg access to certain social networking sites or websites) via the Network Manager. This access may be allowed for some users, at some times, or for a limited period of time. There should be strong educational reasons for changes that are agreed.

Such changes will be agreed with the E-safety Co-ordinator or Headteacher to ensure checks and balances are in place.

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to a teacher (if a pupil) or the Network Manager, who will decide whether to make school level changes (as above).

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School E- Safety Policy and the Acceptable Use Agreement. Monitoring will take place as follows:

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- the ICT technician
- E-Safety co-ordinator
- E-Safety committee
- Local Authority / Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.



Porthcawl Comprehensive School

Personal Data Handling Policy

It is important that the school has a clear and well understood personal data handling policy in order to avoid or at least minimise the risk of personal data breaches. A breach may arise from a theft, a deliberate attack on our systems, the unauthorised use of personal data by a member of staff, accidental loss, or equipment failure. In addition:

- The school or individuals linked to the school would not want to be the cause of any data breach, particularly as the impact of data loss on individuals can be severe and cause extreme embarrassment, put individuals at risk and affect personal, professional or organisational reputation.
- The school is subject to a wide range of legislation related to data protection and data use, with significant penalties for failure to observe the relevant legislation.

Schools have always held personal data on the pupils in their care, and increasingly this data is held digitally and accessible not just in school but also from remote locations. Legislation covering the safe handling of this data is mainly the Data Protection Act 1998 ('the DPA').

It is important to stress that this Personal Data Handling Policy applies to all forms of personal data, regardless of whether it is held on paper or in electronic format. However, as it is part of an overall e-Safety policy, this document will place particular emphasis on data which is held or transferred digitally.

Introduction

Porthcawl Comprehensive School and its employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature.

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office - for the school

and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance..

The DPA lays down a set of rules for the processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and correction. The DPA requires organisations to comply with eight data protection principles, which, among others require data controllers to be open about how the personal data they collect is used.

The DPA defines “Personal Data” as data which relate to a living individual who can be identified

- from those data, or
- from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
- and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

It further defines “Sensitive Personal Data” as personal data consisting of information as to:

- the racial or ethnic origin of the data subject,
- his political opinions,
- his religious beliefs or other beliefs of a similar nature,
- whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- his physical or mental health or condition,
- his sexual life,
- the commission or alleged commission by him of any offence, or
- any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Policy Statements

The school 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”. (see Privacy Notice section below)

Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including *pupils / students*, members of staff and parents / carers eg names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data eg class lists, pupil / student progress records, reports, references
- Professional records eg employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

Responsibilities

The school’s Senior Information Risk Officer roles is shared by the Office Manager Angela Roberts and Deputy Head Jane Sloggett. These people will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school’s information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs)

The school will identify Information Asset Owners (IAOs) (Andrew Slade, Anne O’Brien, Emma Babbage, Luke Rowberry, Ceri-Ann Painter, Britt Henderson, Anne Wallace, Nicola Evans, Caroline Griffiths, Kirsten Morgan and Clair Stephens) for the various types of data being held (eg pupil / student information / staff information / assessment data etc). The IAOs will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose,
- how information has been amended or added to over time, and
- who has access to protected data and why.

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Information to Parents / Carers – the “Privacy Notice”

In order to comply with the fair processing requirements of the DPA, the school will inform parents / carers of all pupils of the data they collect, process and hold on the pupils / students, the purposes for which the data is held and the third parties (eg LA, WG, etc) to whom it may be passed. This privacy notice will be passed to parents / carers via letter. Parents / carers of young people who are new to the school will be provided with the privacy notice with other registration documentation.

Training & awareness

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners
-

Risk Assessments

Information risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present;
- Judging the level of the risks (both the likelihood and consequences); and
- Prioritising the risks.

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions Form (example below):

Risk ID	Information Asset affected	Information Asset Owner	Protective Marking (Impact Level)	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk

Impact Levels and protective marking

Following incidents involving loss of data, the Government recommends that the Protective Marking Scheme should be used to indicate the sensitivity of data. The Protective Marking Scheme is mapped to Impact Levels as follows:

-

Government Protective Marking Scheme label	Impact Level (IL)	Applies to schools?
NOT PROTECTIVELY MARKED	0	Will apply in schools
PROTECT	1 or 2	
RESTRICTED	3	
CONFIDENTIAL	4	Will not apply in schools
HIGHLY CONFIDENTIAL	5	
TOP SECRET	6	

Most pupil or staff personal data that is used within school will come under the PROTECT classification. However some, eg the home address of a child (or vulnerable adult) at risk will be marked as RESTRICT.

The school will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer eg. "Securely delete or shred this information when you have finished using it".

Secure Storage of and access to data

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords which must be changed regularly. User passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media (**where allowed**)). Private equipment (ie owned by the users) must not be used for the storage of personal data.

When personal data is stored on any portable computer system, USB 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 and
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

The school has clear policy and procedures for the use of “Cloud Based Storage Systems” (for example Office365) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

As a Data Controller, the school is responsible for the security of any data passed to a “third party”.

All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.

The school recognises that under Section 7 of the Data Protection Act, <http://www.legislation.gov.uk/ukpga/1998/29/section/7> data subjects have a number of rights in connection with their personal data, the main one being the right of access. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure;
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation’s premises (for example, by a member of staff to work from their home), they will have secure remote access to the management information system or learning platform;
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event.

Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance and other media must be shredded, incinerated or otherwise disintegrated for data.

Audit Logging / Reporting / Incident Handling

It is good practice that the activities of data users, in respect of electronically held personal data, will be logged and these logs will be monitored by responsible individuals.

The audit logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy, for example.

The school has a procedure for reporting, managing and recovering from information risk incidents, which establishes:

- a “responsible person” for each incident;
- a communications plan, including escalation procedures;
- and results in a plan of action for rapid resolution; and
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner’s Office based upon the local incident handling policy and communication plan.

Use of technologies and Protective Marking

The following provides a useful guide:

	The information	The technology	Notes on Protect Markings (Impact Level)
School life and events	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events	Common practice is to use publically accessible technology such as school websites or portal, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.
Learning and achievement	Individual pupil / student academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs.	Typically schools will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent.	Most of this information will fall into the PROTECT (Impact Level 2) category. There may be students/pupils whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the school may decide not to make this pupil / student record available in this way.
Messages and alerts	Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	Email and text messaging are commonly used by schools to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via "dashboards" of information, or be used to provide further detail and context.	Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts about schools closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.

Use of Cloud Services

The movement towards tablet and other mobile technologies in schools presents both opportunities as well as challenges. Ultimately, the opportunities are around teaching and learning; the challenges are around successfully managing this pedagogical shift and taking staff, parents and pupils through this technological change. At the heart of the change is a move away from devices or systems where information is stored locally, to devices which can access data stored 'in the cloud'. Just as a PC needs to be connected

to a network to get to the stored data, so must these mobile and tablet devices be connected to the cloud. Wireless access provides this connection.

Software too can sit in the cloud removing the need for locally installed suites of software. Apps offer an opportunity to create low cost, flexible learning opportunities which are device agnostic and which can create personalised learning on a new level.

Using the Hwb+ learning platform the school has been provisioned with Office 365 which offers cloud based email, calendar and storage facilities as well as MS Office. By it's nature, Office 365 is available on any device which is connected to the internet meaning that these cloud based services can be accessed in school or at home on smartphones, tablets, laptops, notebooks and PCs.

Just as a school has obligations around data on its physical network, the same obligations are required when dealing with data in the cloud i.e. it is still required to be protected in line with the Data Protection Act (DPA) and may be subject to Freedom of Information (FOI) requests.

Freedom of Information

FOI may require anything you write in an official capacity to be potentially made public.

Data Protection Act

Schools, like any other organisation, are subject to the Data Protection Act (DPA) and its eight basic principles. The DPA refers to 'personal data' – this can be described generally as information which identifies an individual and is personal to an individual.

The DPA contains eight 'Data Protection Principles' which specify that personal data must be:

- Processed fairly and lawfully
- Obtained for specified and lawful purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept any longer than necessary
- Processed in accordance with the 'data subject's' (the individual's) rights
- Securely kept
- Not transferred to any other country without adequate protection

It's also worth considering that whilst not all data is 'personal', the information that is, has varying levels of sensitivity based on the impact were it to be compromised.

Safeguarding

There are also safeguarding obligations for the use of technology in schools that include:

-

- Effectively monitoring the use of systems to detect potential and actual safeguarding issues
- Monitoring, alerting and responding to illegal activity
- Providing consistent safeguarding provision both within and beyond school if devices/services leave the site

Criminal Activity

Schools have an immediate obligation to report illegal or criminal activity to the Police. Other services e.g. Facebook, Twitter, etc are useful cloud tools in and beyond the classroom but it is important to be aware of age restrictions here too. US Law requires any company operating within the US to comply with the Children's Online Privacy Protection Act (COPPA) which legislates against companies who store, process and manage information on children aged 13 and under and the active or targeted marketing to that age group.

Security concerns

Access to data through devices is much more likely given that devices are going to and from school in bags, on buses, or left lying around at home or school so security now becomes much more of an issue at a user level than it ever has before. If a device goes missing or breaks, the big advantage of cloud systems is that, apart from simple local settings, content is in the cloud so data is not 'lost' in the same way as if your laptop was stolen or suffers a hard drive failure.

Passwords and authentication are critical at any point in securing access to data but are especially so with data in the cloud. Therefore passwords must be strong and changed regularly.

Monitoring users

Local networks based on site have the advantage of being relatively easy to filter and monitor for inappropriate or illegal use and the school has effective systems in place

Microsoft state in their user agreements that they reserve the right to actively search stored files.

This means that the school also needs to be clear about what the expectations are around illegal and inappropriate content and how it intends to ensure those expectations are met. These include:

- Clear and effective agreement through Acceptable Use Agreements
- Positive statements and posters around the use of technology dotted around school in areas where that technology might be used
- Active education in raising awareness of what illegal or inappropriate both mean
- Staff development in recognising and escalating reports of illegal content
- Reminders that Cloud Service Providers can and do scan content stored on their servers and that an archive exists

- Establish regular spot checks on mobile devices and advertise the fact that these will be carried out on school devices and removable media
- Establish and communicate that One Drives provided as part of a school cloud solution will be subject to random spot checks by resetting passwords back to default to allow auditing or by the expectation that users should share their online folders with their teacher. The system has been provided for educational use so there should not be anything in there that isn't related to learning.

Freedom of Information Act

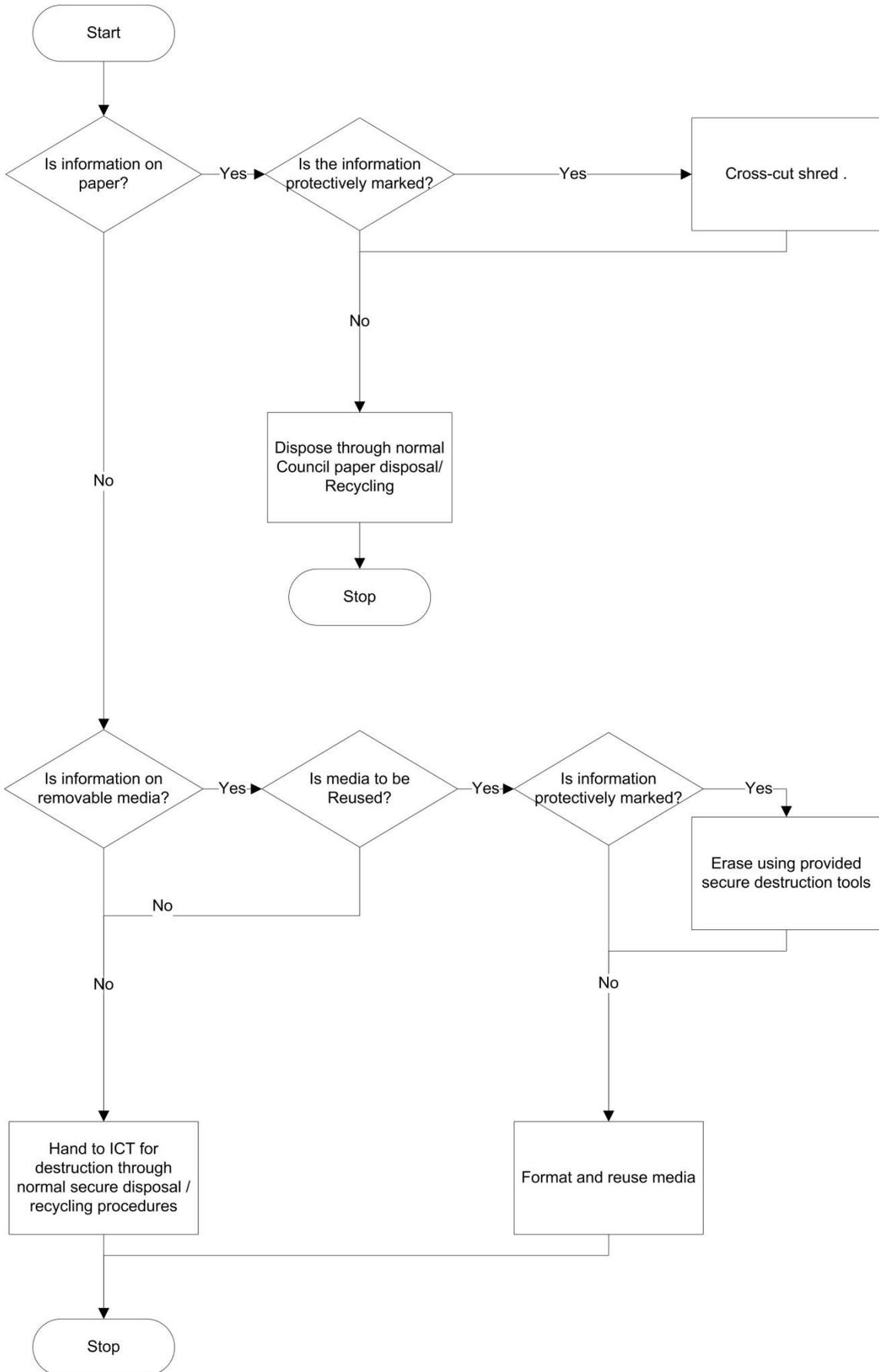
The school has a Freedom of Information Policy (from BCBC) which sets out how it will deal with FOI requests. In this policy the school:

- Delegates to the Headteacher responsibility for FOIA policy and the provision of advice, guidance, publicity and interpretation of the school's policy.
- Considers arrangements for overseeing access to information and delegation to the appropriate governing body.
- Ensures that a well managed records management and information system exists in order to comply with requests.
- Ensures a record of refusals and reasons for refusals is kept, allowing the Governing Body to review its access policy on an annual basis.

BCBC Information Transmission Guidance

Action	Information Classification		
	NPM	PROTECT	RESTRICT
Paper delivery by hand to verified internal recipient.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Paper delivery by hand to verified external recipient requiring data as part of role.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Removable media delivery by hand to verified internal recipient where media is encrypted.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Paper or removable media delivery by sealed internal mail.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Paper or removable media delivery by sealed internal mail.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Paper or removable media delivery by unsealed internal mail	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Paper or removable media delivery by secure courier to UK/EU destinations	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Paper or removable media delivery by standard post to UK/EU destinations	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Facsimile to UK/EU destinations following secure procedure below	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Facsimile to UK/EU destination	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delivery via GCSx email internally	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Delivery via GCSx email externally to a registered GSI/GCSx/PNN etc. destination	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Delivery via non-GCSx email internally	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delivery via non-encrypted email externally to UK/EU destinations	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Across internal network, where user has had MARK training	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Across internal network where user has not had MARK training, with exception recorded by data sender	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Across internal from external places designated for home working to BCBC network (e.g. VPN), terminated at a BCBC device.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
To suppliers on encrypted media, where the release is require for business purposes and the exception recorded.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Across any other link to BCBC network.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

BCBC Information Disposal Guidance



Appendix B3

Bring Your Own Device Acceptable Use Policy (BYOD AUP)

Porthcawl Comprehensive School recognises that as technology advances students & staff are able to access more internet capable devices. This should be seen as a resource and provide the opportunity to enable quick and easy access to materials online allowing enhanced learning.

General Information

Access to Porthcawl Comprehensive's wireless network, whether with school-provided equipment or a personal device, is filtered in compliance with the Computer Misuse Act (CMA) & BCBC Internet Access for Schools Policy. However, access from a personal device is limited to internet use only. Students & staff will not have access to any resources which reside on the school network from their personal device.

Access to Porthcawl Comprehensive's wireless network is a privilege, not a right. Any use of the wireless network entails personal responsibility and compliance with all school rules. The use of the network also allows ICT Support staff to conduct investigations regarding inappropriate internet use at any time, by Senior Management request.

Obtaining Access to the Network

To obtain access to the network staff or students/parental guardian will need to sign this policy which states that they have read and understand the terms. Workshops will be held in the Library at Lunch Times on dates provided by the Senior ICT Technician.

To allow devices to connect to SSL protected sites (https://) the user will need to install a special certificate for SSL Inspection. This will be provided in the workshop.

Guidelines for Use

- Use of personal devices during the school day is at the discretion of the teachers and support staff. Students must use devices as directed.
- The primary purpose of the use of personal devices at school is educational. Using the devices for personal reasons e.g. contacting parents, should only take place after permission has been given from a teacher or other member of support staff.
- The use of a personal device is not to be a distraction in any way to staff or students. Personal devices must not disrupt class in anyway.
- Personal devices can be used at break or lunch for recreational purposes but should still adhere to the BYOD & ICT policy.
- Students & staff will make no attempt to circumvent the school's network security and/or filtering policies. This includes setting up proxies and downloading programs to bypass security.
- Students & staff shall not distribute pictures or videos of students or staff without permission (distribution can be as small as emailing/texting to one other person or as large as posting image or video online).

Consequences for Misuse/Disruption

(One or more may apply):

- Access to the wireless network will be removed.
- Devices may be confiscated for a period of time. (Devices will be kept in A Block in a locked safe.)
- Student or Staff member will be denied use of personal devices at school.
- Internet access will be removed.

Serious misuse of Internet capable devices is regarded as a serious offence and will be dealt with in accordance to the schools Behaviour Management Policy. Inappropriate use of internet access such as attempting to enter adult, terror and copyrighted content (torrenting) sites will be recorded and could be provided as evidence to the police should the need arise.

School Liability Statement

Students & staff bring their devices to use at Porthcawl Comprehensive School at their own risk. Students & Staff are expected to act responsibly with regards to their own device, keeping it up to date and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices.

Porthcawl Comprehensive School is in no way responsible for:

- Personal devices that are broken while at school or during school-sponsored activities.
- Personal devices that are lost or stolen at school or during school-sponsored activities.
- Maintenance or upkeep of any device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues).

I hereby sign this form stating that I have read and understand the contents and will agree to abide by this policy.

Student's Signature: _____ Student's Print Name: _____

Curriculum Username: _____ E.g. 10BLOGSJ

Parental / Guardian Signature: _____ Date: _____



Porthcawl Comprehensive School

Social Media Policy

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

Porthcawl Comprehensive School recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils/students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by Porthcawl Comprehensive School, its staff, parents, carers and children.

Scope

This policy is subject to the school's Codes of Conduct and Acceptable Use Agreements.

This policy:

- **Applies to all staff and to all online communications which directly or indirectly, represent the school.**
- **Applies to such online communications posted at any time and from anywhere.**
- Encourages the safe and responsible use of social media through training and education
- Defines the monitoring of public social media activity pertaining to the school

The school respects privacy and understands that staff and pupils/students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Digital communications with pupils/students are also considered. *Staff may use social media to communicate with learners via a school social media account for **teaching and learning** purposes but must consider whether this is appropriate and consider the potential implications.*

Roles & Responsibilities

- **Senior Leadership Team**
 - Facilitating training and guidance on Social Media use.
 - Developing and implementing the Social Media policy
 - Taking a lead role in investigating any reported incidents.
 - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
 - Receive completed applications for Social Media accounts
 - Approve account creation
- **Senior ICT Technician**
 - Create the account following SLT approval
 - Store account details, including passwords securely
 - Be involved in monitoring and contributing to the account
 - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)
- **Staff**
 - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
 - Attending appropriate training
 - Regularly monitoring, updating and managing content he/she has posted via school accounts
 - Adding an appropriate disclaimer to personal accounts when naming the school

Managing accounts

- **Process for creating new accounts**

The school community is encouraged to consider if a social media account will help them in their work, eg a history department Twitter account, or a "Friends of the school" Facebook page. Anyone wishing to create such an account must present a business case in writing to the School Leadership Team which covers the following points:-

 - The aim of the account
 - The intended audience
 - How the account will be promoted
 - Who will run the account (at least two staff members should be named)
 - Will the account be open or private/closed

Following consideration by the Senior Leadership Team an application will be approved or rejected. In all cases, the Senior Leadership Team must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

- **School accounts must be monitored regularly and frequently** (preferably also during holidays). Any comments, queries or complaints made through those accounts must be responded to in line with the school's Complaints Policy and procedures. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour

- **The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.**

- **Digital communications by staff must be professional and respectful at all times and in accordance with this policy.** Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts could not be made in relation to school activity.
- If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. *Where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken*
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- **Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.**
- **Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.**

Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Tone

- The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:
 - Engaging
 - Conversational
 - Informative
 - Friendly (on certain platforms, eg. Facebook)

Use of images

- School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.
 - **Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy.** If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
 - **Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts**
 - Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
 - If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

- **Staff**
 - Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
 - Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
 - Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
 - **Staff are not permitted to follow or engage with current pupils/students of the school on any personal social media network account.**
- **Pupil/Students**
 - The school's education programme should enable the pupils/students to be safe and responsible users of social media.
 - Pupils/students are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy
- **Parents/Carers**
 - **If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.**
 - The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
 - Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes the school's Social Media Policy sets out clear guidance for staff to manage risk and behaviour online. Core to our behaviour is the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out by the Education Workforce Council (EWC) 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 Porthcawl Comprehensive School 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 e-Safety Coordinator/Officer, Senior ICT Technician and e-Safety committee to ensure compliance with the school's Social Media, Data Protection, and Digital Images and Video Policies.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying 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 students / 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 eg 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 students / 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 and guidelines concerning the sharing, distribution and publication of those images. (Social Media Policy, Code of Safe Practice, Data Security Good Practice Guide and Protocol for the Use of Social Media). 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 students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- **Students' / 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 students / pupils are published on the school website or Twitter as part of the Acceptable Usage Agreement signed by parents or carers at the start of the year.
- Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.

Appendix

Managing your personal use of Social Media:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

Managing school social media accounts:

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Consider turning off tagging people in images where possible

The Don'ts

- Don't make comments, post content or link to materials that will bring the school into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

Acknowledgements

With thanks to Rob Simmonds of Well Chuffed Comms (wellchuffedcomms.com) and Chelmsford College for allowing the use of their policies in the creation of this policy.

Copyright of the SWGfL School Online Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.



Application for school Social Media account

Department: _____

Type of account proposed: _____

Aim of the account:

Intended audience:

How the account will be promoted?

Who will run the account? (at least two staff members should be named)

- _____
- _____
- _____

Will the account be open or private/closed? _____

In applying to run this account you acknowledge that you have read and agree with school's Social Media Policy.

Signed: 1. _____ 2. _____ 3. _____

Date: _____

.....

Approved

Declined

Signed: _____ Headteacher

Date: _____

If approved you must provide details of the account to the Senior ICT Technician, including passwords.



Porthcawl Comprehensive School

e-Safety Group Terms of Reference

1. PURPOSE

To provide a consultative group that has wide representation from the school community, with responsibility for issues regarding e-Safety and the monitoring of the e-Safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

2. MEMBERSHIP

2.1 The e-Safety committee will seek to include representation from all stakeholders. The composition of the group should include

- SLT member/s
- Safeguarding officer
- Teaching staff member
- Support staff member
- e-Safety coordinator
- Governor
- Parent / Carer
- ICT Technical Support staff
- Community users
- Student / pupil representation – for advice and feedback. *Student / pupil voice is essential in the make up of the e-Safety committee, but students / pupils would only be expected to take part in committee meetings where deemed relevant.*

2.2 Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

2.3 Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.4 Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature

2.5 When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities.

3. CHAIRPERSON

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members;
- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;

- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary.

4. DURATION OF MEETINGS

Meetings shall be held once every half term. A special or extraordinary meeting may be called when and if deemed necessary.

5. FUNCTIONS

These are to assist the e-Safety Co-ordinator (or other relevant person) with the following:

- To keep up to date with new developments in the area of e-Safety
- the production / review / monitoring of the school e-Safety policy / documents in line with new technologies and incidents
- To monitor the delivery and impact of the e-Safety policy
- To monitor the log of reported e-Safety incidents to inform future areas of teaching / learning / training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of e-Safety
- Mapping and reviewing the e-Safety curricular provision – ensuring relevance, breadth and progression
- Monitoring improvement actions identified through use of the 360 degree safe Cymru self review tool
- To ensure that monitoring is carried out of Internet sites used across the school (if possible)
- To monitor filtering / change control logs (e.g. requests for blocking / unblocking sites).
- To monitor the safe use of data across the school
- To monitor incidents involving cyberbullying for staff and pupils

This could be carried out through:

- Staff meetings
- Student / pupil forums (for advice and feedback)
- Governors meetings
- Surveys/questionnaires for students / pupils, parents / carers and staff
- Parents' Evenings
- Website/VLE/Newsletters
- e-Safety events
- Internet Safety Day (annually held on the second Tuesday in February)
- Other methods

6. AMENDMENTS

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority

The above Terms of Reference for Porthcawl Comprehensive School have been agreed

Signed by (SLT):

Date:

Date for review:

Appendix C1

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

--

Web site(s) address / device

Reason for concern

Web site(s) address / device	Reason for concern

Conclusion and Action proposed or taken

Appendix C3

Summary of Legislation

Schools should be aware of the legislative framework under which this e-Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- “Eavesdrop” on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

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

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject’s rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

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

Communications Act 2003

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

Malicious Communications Act 1988

It is an offence to send an indecent, grossly offensive, or threatening letter, electronic communication or other article to another person. It is also an offence to send information which is false and known or believed to be false by the sender.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Where the system controller has given express consent monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.

Trade Marks Act 1994

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

Copyright, Designs and Patents Act 1988

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

Criminal Justice & Public Order Act 1994 / Public Order Act 1986

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

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006 / Public Order Act 1986

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

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.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence is liable to imprisonment for a term of not more than 10 years, or to a fine or to both.

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. (Typically, teachers, social workers, health professionals, connections staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

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

Obscene Publications Act 1959 and 1964

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

Human Rights Act 1998

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

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression

- Freedom of assembly
- Prohibition of discrimination
- The right to education
- The right not to be subjected to inhuman or degrading treatment or punishment

The school is obliged to respect these rights and freedoms, but should balance them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

Appendix C4

Links to other organisations or documents

The following links may be of interest to those reading or reviewing the school E-Safety policy.

UK Safer Internet Centre

- [Safer Internet Centre](#)
- [South West Grid for Learning](#)
- [Childnet](#)
- [Professionals Online Safety Helpline](#)
- [Internet Watch Foundation](#)

CEOP

- <http://ceop.police.uk/>
- [ThinkUKnow](#)

Others

- INSAFE - <http://www.saferinternet.org/ww/en/pub/insafe/index.htm>
- UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis
- Netsmartz - <http://www.netsmartz.org/index.aspx>

Support for Schools

- Specialist help and support - [SWGfL BOOST](#)

Cyberbullying

- Scottish Anti-Bullying Service, Respectme - <http://www.respectme.org.uk/>
- Scottish Government - [Better relationships, better learning, better behaviour](#)
- [Welsh Government – Respecting Others](#)
- Anti-Bullying Network - <http://www.antibullying.net/cyberbullying1.htm>
- Cyberbullying.org - <http://www.cyberbullying.org/>

Social Networking

- Digizen – [Social Networking](#)
- [SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people](#)
- [Connectsafely Parents Guide to Facebook](#)
- [Facebook Guide for Educators](#)

Curriculum

- [SWGfL Digital Literacy & Citizenship curriculum](#)
- Alberta, Canada - [digital citizenship policy development guide.pdf](#)
- Teach Today – www.teachtoday.eu/
- Insafe - [Education Resources](#)

- Somerset - [e-Sense materials for schools](#)

Mobile Devices / BYOD

- Cloudlearn Report [Effective practice for schools moving to end locking and blocking](#)
- NEN - [Guidance Note - BYOD](#)

Data Protection

- Information Commissioners Office:
 - [Your rights to your information – Resources for Schools - ICO](#)
 - [ICO pages for young people](#)
 - [Guide to Data Protection Act - Information Commissioners Office](#)
 - [Guide to the Freedom of Information Act - Information Commissioners Office](#)
 - [ICO guidance on the Freedom of Information Model Publication Scheme](#)
 - [ICO Freedom of Information Model Publication Scheme Template for schools \(England\)](#)
 - [ICO - Guidance we gave to schools - September 2012 \(England\)](#)
 - [ICO Guidance on Bring Your Own Device](#)
 - [ICO Guidance on Cloud Hosted Services](#)
 - [Information Commissioners Office good practice note on taking photos in schools](#)
 - [ICO Guidance Data Protection Practical Guide to IT Security](#)
 - [ICO – Think Privacy Toolkit](#)
 - [ICO – Personal Information Online – Code of Practice](#)
 - [ICO – Access Aware Toolkit](#)
 - [ICO Subject Access Code of Practice](#)
 - [ICO – Guidance on Data Security Breach Management](#)
- SWGfL - [Guidance for Schools on Cloud Hosted Services](#)
- LGfL - [Data Handling Compliance Check List](#)
- Somerset - [Flowchart on Storage of Personal Data](#)
- NEN - [Guidance Note - Protecting School Data](#)

Professional Standards / Staff Training

- DfE - [Safer Working Practice for Adults who Work with Children and Young People](#)
- Kent - [Safer Practice with Technology](#)
- Childnet / TDA - [Social Networking - a guide for trainee teachers & NQTs](#)
- Childnet / TDA - [Teachers and Technology - a checklist for trainee teachers & NQTs](#)
- [UK Safer Internet Centre Professionals Online Safety Helpline](#)

Infrastructure / Technical Support

- Somerset - [Questions for Technical Support](#)

- NEN - [Guidance Note - esecurity SWGfL / Common Sense Media Digital Literacy & Citizenship Curriculum](#)

Working with parents and carers

- [SWGfL BOOST Presentations - parents presentation](#)
- [Connect Safely - a Parents Guide to Facebook](#)
- [Vodafone Digital Parents Magazine](#)
- [Childnet Webpages for Parents & Carers](#)
- [DirectGov - Internet Safety for parents](#)
- [Get Safe Online - resources for parents](#)
- [Teach Today - resources for parents workshops / education](#)
- [The Digital Universe of Your Children - animated videos for parents \(Insafe\)](#)
- [Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide](#)
- [Insafe - A guide for parents - education and the new media](#)
- [The Cybersmile Foundation \(cyberbullying\) - advice for parents](#)

Research

- [EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011](#)
- [Futurelab - "Digital participation - its not chalk and talk any more!"](#)

Appendix C5

Glossary of terms

AUA	Acceptable Use Agreement
CAIC list	Child Abuse Image Content List
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes).
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
FOSI	Family Online Safety Institute
EA	Education Authority
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom regulator)	Office of Communications (Independent communications sector
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational e-Safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting.
WAP	Wireless Application Protocol