Policy for:

Safe use of Internet and E-Safety Policy 2026-28

Committee: Headteacher

Document Control

A. Confidentiality Notice

This policy document has been approved by the Headteacher of St.Modwen's Catholic Primary School and is intended for internal and /or external publication. Where the document is identified for internal use the policy information may not be shared with external agencies or parents without the prior agreement of the Headteacher or authorising Committee.

B. Document Details

Classification:	Headteacher/SMT
Policy Source:	School Policy
Organisation:	St. Modwen's Catholic Primary School
Document Reference:	STM20
Current version number:	26.28 V2 (20 pages)
Current Document Approved by:	Headteacher
Date Approval:	February 2026
Scheduled Review:	February 2028 (2 Years)

C. Document Revision and Approval History

Version	Date	Version Created by	Version Approved by	Comments
Version 2	13.2.2026	C Salt (SBM)	Headteacher	School Amends: Page 3: DPO - DPO (phplaw); Policy dates (Bi-annually) KCSIE current version (page 3)
Version 1	20.1.2024	C Salt (SBM)	Premises, Health & Safety	School Policy Insert Front Sheet GDPR Policy review, Working Together to Safeguard Children 2023; E Safety Act 2023 . and KCSIE 2023 (page 3) Knowsley On-line safety page 9

Contents

1. **Policy Review and Links to other School Policies**

2. **Scope of the Policy**

3. **Rules to help us to be fair to others and keep everyone safe**

4. **Roles and Responsibilities**
   - Governors
   - Headteacher and Senior Leaders
   - E-Safety Coordinator (DSP) & Computing Subject Leader
   - Network Manager / Technical staff
   - Teaching and Support Staff
   - Child Protection / Safeguarding Designated Person
   - Pupils
   - Parents / Carers
   - Community Users

5. **Policy Statements**
   - Education – pupils
   - Education – parents / carers
   - Education – The Wider Community
   - Education & Training – Staff / Volunteers
   - Training – Governors
   - Technical – infrastructure / equipment, filtering and monitoring
   - Bring Your Own Device (BYOD)
   - Use of digital and video images
   - General Data Protection Regulation (GDPR) 2018
   - Communications
   - Social Media
   - Protecting Professional Identity
   - Unsuitable / inappropriate activities
   - Responding to incidents of misuse
   - Illegal Incidents
   - Other Incidents
   - School Actions & Sanctions

1. Policy Review and Links to other School Policies

This e-safety policy was approved by the *Headteacher:*	**February 2026**
• The implementation of this e-safety policy will be monitored by the:	*SLT*
• Monitoring will take place at regular intervals:	*Bi-Annually*
• The *Governing Body* will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	*Annually*
The E-Safety Policy will be reviewed biannually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	**February 2028**

Should serious e-safety incidents take place, the following external persons / agencies should be informed:

- Headteacher/School Information Security Lead
- DPO (phplaw)
- ICO
- CEOP (reference Flow chart)

NB. This policy replaces the Safe use of Internet/E-Safety Policy approved and published. Please also reference School safeguarding policies

Links to other school GDPR policies

GDPR School Policies	Review Date
01 Data Protection Policy	September - Annually
02 Breach and Non Compliance Policy	September - Annually
03 Confidentiality Policy and Confidential Agreements	September - Annually
04 CCTV Policy	September - Annually
05 Workforce Acceptable use Policy	September - Annually
06 Freedom of Information Policy	September - Annually
07 Document and Data Retention Policy	September - Annually
08 Privacy Notices: Pupils Data School Trips Staff Workforce Governors Job Applicants	September - Annually
09 GDPR Workforce and Governor Training/CPD	September - Annually
10 GDPR Checks, Compliance and Audit Toolkit (GoGDPR)	September - Annually
11 GDPR Subject Access Request Management and Procedures	September - Annually
12 GDPR My rights a guide for data subjects	September - Annually

Links to School Safeguarding Policies and Practice

This document is a statement of the schools commitment to ensuring Safe Use of the Internet at St Modwen's. This policy also runs in conjunction with our Safeguarding, Anti-Bullying and Behaviour

policies. Staff at St Modwen's are all expected to work in accordance with the 'Safer Working Practice Guidance 'Safeguarding: All staff plan their learning for pupils in this subject by adhering to the guidelines laid out in the latest version of 'Keeping Children Safe in Education.; On-Line Safety Act All staff are trained and told to adhere to the 'Working Together to Safeguard Children 2023.

This Policy covers all offline and online activity by the same principles and is used in conjunction with our related policies for Equal Opportunities, Disability Access Arrangements, SEN and Inclusion, Racial Equality and Harassment, Catholic Life (including Prevent strategies and SMSC) and the schools 'Positive Behaviour Policy/Code of Conduct.

Links to School Disability Equality Impact Assessment
This policy has been written with reference to and in consideration of the school's Disability Equality Scheme. Assessment will include consideration of issues identified by the involvement of disabled children, staff and parents and any information the school holds on disabled children, staff and parents.

Any questions or concerns regarding this policy should be made to The Head Teacher or Deputy Head Teacher.

The school will monitor the impact of the policy using Logs of reported incidents and Surveys / questionnaires of students / pupils, parents / carers and staff.

2. Scope of the Policy

This policy applies to all members of the school (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.

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

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

Aims: Our aims in writing a policy for Safe Access to the Internet are to ensure that:-

- All members of the school community – children, teachers, parents and governors – are aware of the need for safe and responsible internet use
- The issues surrounding internet safety are discussed
- Internet use supports schools' educational aims
- LA requirements are satisfied.

What is the need for Internet Access at school?

- School internet use is now an important part of teaching, learning, administration and communication
- It makes possible a wider range of information, the scope and nature of which may or may not be appropriate
- Used responsibly it can raise educational standards, support the professional work of staff and to enhance the school's management information and business administration systems.
- It is a beneficial learning tool when children have been taught to understand its value and limitations.

How can the Internet be used as a teaching and learning tool?

Teachers, parents and children should be able to develop good practice in using the Internet as a tool for teaching and learning. We believe that:-

- Internet access will enrich and extend learning activities.
- On-line activities that will support the learning outcomes planned for the children's age and maturity.
- Children should be confident using the Internet for research, including the skills of knowledge location, retrieval and evaluation of material found.

What are the benefits?

Benefits of internet access at Primary level include:

- Access to world-wide educational resources including museums and art galleries
- Educational and cultural exchanges between children worldwide
- Cultural, vocational, social and leisure use in libraries, clubs and at home
- Access to experts in many fields for children and staff
- Staff professional development through access to national developments
- Educational materials and good curriculum practice
- Communication with support services, professional associations and colleagues
- Improved access to technical support including remote management of networks
- Exchange of curriculum and administration data with the LA and DfE.

How will children be taught to assess Internet content responsibly?

- Children will be taught ways to validate information before accepting it is necessarily accurate
- Children will be taught to acknowledge the source of information, when using Internet material for their own use.
- Children will be made aware that the writer of an email or the author of a Web page might not be the person claimed.
- Children will be encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

How will staff and children be consulted?

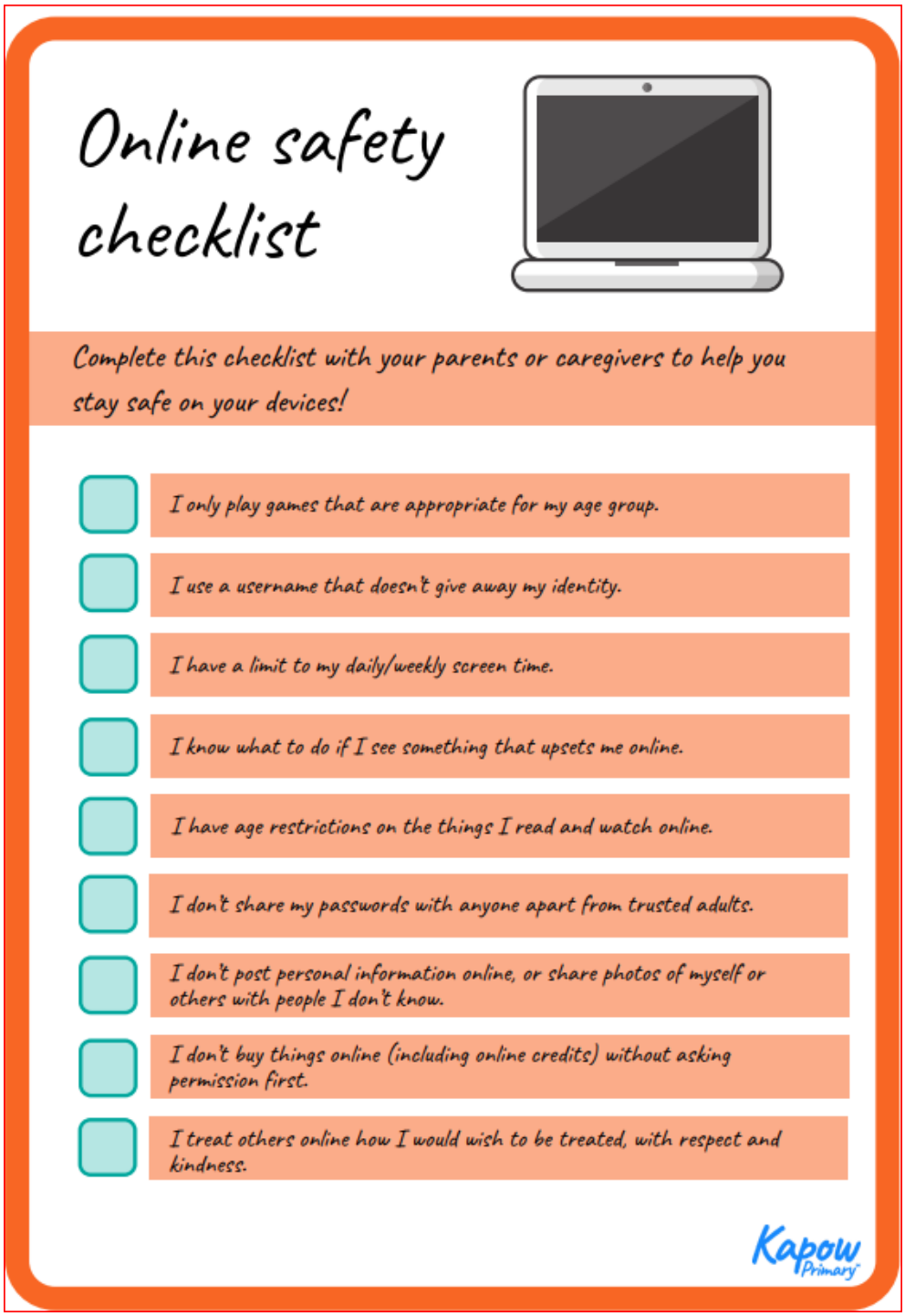
- Rules for Safe Use of Internet access will be discussed with children through School Parliament, whole school assemblies, class discussions and information posted near the computer storage area in the library and in classrooms.
- All staff including teachers, supply staff, classroom assistants and support staff and parents will be made aware these rules, and their importance explained
- Parents' attention will be drawn to the Policy in newsletters, the school prospectus and on the school Web site and parents will be asked to sign to say they have seen a copy of it.
- A unit on responsible Internet use will be included every half term and when situations arise that require discussion especially during Anti-Bullying Week and in SRE lessons designed to ensure that pupils from the age of 10+ understand that they are criminally culpable for inappropriate online activity.

How will parent's support be enlisted?

The school believes it has a duty to help parents plan appropriate use of the Internet at home, and as such:-

- A careful balance between informing and alarming parents will be maintained
- Joint home/school guidelines on issues such as safe Internet use will be established
- Parents will be invited to school to take part in an internet safety workshop each year
- Suitable educational and leisure activities that make responsible use of the Internet will be developed with parents.

3.Rules to help us to be fair to others and keep everyone safe.



The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be taking place, or the system is or may be used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Be smart on the internet

Childnet International
www.childnet.com

S SAFE Keep safe by being careful not to give out personal information when chatting or posting online. Personal information includes your email address, phone number and password.

M MEETING Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time.

A ACCEPTING Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

R RELIABLE Someone online might lie about who they are, and information on the internet may not be true. Always check information with other websites, books or someone who knows.

T TELL Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

You can report online abuse to the police at www.thinkuknow.co.uk

www.kidsmart.org.uk

KidSMART

Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.

4. Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

Governors: are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about e-safety incidents and monitoring reports. A member of the *Governing Body* has taken on the role of *E-Safety Governor*. The role of the E-Safety *Governor* will include:

- regular meetings with the E-Safety Co-ordinator & Computing Subject Lead
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors / Board / committee / meeting

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e- safety allegation being made against a member of staff or member of the school community
- The Headteacher and Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

E-Safety Coordinator (DSP) & Computing Subject Leader (e-safety network team)

- leads the e-safety committee- meeting on regular basis to discuss e-safety issues
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the recording procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e- safety developments
- meets regularly with E-Safety *Governor* to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of *Governors*
- reports regularly to Senior Leadership Team

Network Manager / Technical staff: The *Computing* Lead is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack that the school meets required e-safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person

- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Senior Leader; E-Safety Coordinator.

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school / school e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher & e-safety network team for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the e-safety and acceptable use policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned 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. Each of these sessions are to include a recap of e-safety requirements

Child Protection / Safeguarding Designated Person should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying. (Reference Mobile Phone Policy)
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school. Pupils must understand that any e-safety issues that occur outside of school will still be dealt with by the school.

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The *school* will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature.* Parents and carers will be encouraged to support the *school* in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- Knowsley On-Line resource subscription which includes on-line Newsletters for parents
- National College resource subscription – access to webinars, updates and training courses for parents
- access to parents' sections of the website
- their children's personal devices in the school (where this is allowed)

Community Users who access school systems / website as part of the wider *school* provision will be expected to sign a Community User AUA before being provided with access to school systems.

6. Policy Statements

Education – pupils

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 *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 Computing / PHSE/ other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students / pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit. It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) 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. Any request must be recorded on appropriate request form and retained by the e-safety network team.

Education – parents / carers

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

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

- Curriculum activities
- Letters, newsletters, website
- Safeguarding Policy
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications
- Attend e-safety assemblies and support sessions

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's e-safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and e-safety
- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- The School website will provide e-safety information for the wider community supporting community groups eg Early Years Settings, Childminders, youth / sports /voluntary groups to enhance their e-safety provision

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 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 or Computing Leader will receive regular updates through attendance at external training events (eg from LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Coordinator / Officer or Computing Subject Lead will provide advice /
- guidance / training to individuals as required.

Training – Governors

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

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation
- Participation in school training / information sessions for staff

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 need to 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 /school meets recommended technical requirements
  There will be regular reviews and audits of the safety and security of school school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school / school technical systems and devices.
- The Headteacher / Computing Leader 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.
- School / 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 (to be described) 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.
- An agreed policy is in place for the provision of temporary access of "guests" (eg
- trainee teachers, supply teachers, visitors) onto the school systems.

- Personal data cannot 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 exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the GDPR 2018 principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's / school's normal
- filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Pupils receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Any user leaving the school will follow the process outlined within the BYOD policy

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for 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 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 in not covered by the GDPR 2018). 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.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents or carers and will only be used by the School.

General Data Protection Regulation (GDPR) 2018

Personal data will be recorded, processed, transferred and made available according to the GDPR (2018) which states that personal data must be:

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

The school must ensure that:

Main Changes	How we are complying with changes
1. School must appoint DPO, advise on compliance and other relevant data protection law	John Walker Solicitor John@phplaw.co.uk
2. Privacy notices must be in clear and plain language and include extra information – the school's 'lawful basis' for processing the individual's rights in relation to own data	Reference: Privacy Notices for pupils and parents Privacy Notices for staff workforce
3. School will only have 1 month to comply with subject access requests, and in most cases can't charge	Reference: Section 8:Data Sharing Policy Section 7 and Appendix 2 : Data Protection Policy
4. Where the school needs an individual's consent to process data, this consent must be freely given, specific, informed and unambiguous	Consent forms revised June 2018 Withdrawal Consent forms developed August 2018
5. Schools will need to carry out a data protection impact assessment when considering using data in new ways, or implementing new technology to monitor pupils	Reference: Privacy Impact Assessments (PIA) Section 8 and Appendix 3: Data Protection Policy
6. Schools will have to demonstrate how they comply with the new law	Reference School Policies and Planning documents introduced A1 Term 2018
7. There are new, special protections for children's data with regard to online services	
8. Higher fines for data breaches – up to 20 million euros	

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/sensitive data.
- Transfer data using encryption and secure password protected devices.

Communications

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

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

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users must immediately report, to the nominated person – in accordance with the school / 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) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Staff must not accept social media requests from children or parents in the school community.

- Whole class / group email addresses may be used at KS1, while student pupils at KS2 will be provided with individual school email addresses for educational use.
- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media

Use of Social networking sites in worktime

Use of social networking applications in work time for personal use only is **not permitted**, unless permission has been given by the Head teacher.

Social Networking as part of School Service

All proposals for using social networking applications as part of a school service (whether they are hosted by the school or by a third party) must be approved by the Head teacher first.

Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct. St.Modwen's Catholic Primary School School expects that users of social networking applications will always exercise the right of freedom of expression **with due consideration for the rights of others** and strictly in accordance with School Workforce Acceptable use of IT Policy

Protecting Professional Identity

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, politics 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 incidents of e-safety breach must be recorded on the e-safety Incident Report Form and retained by the Online Safety Officer.

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 pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

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

Unsuitable / inappropriate activities

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

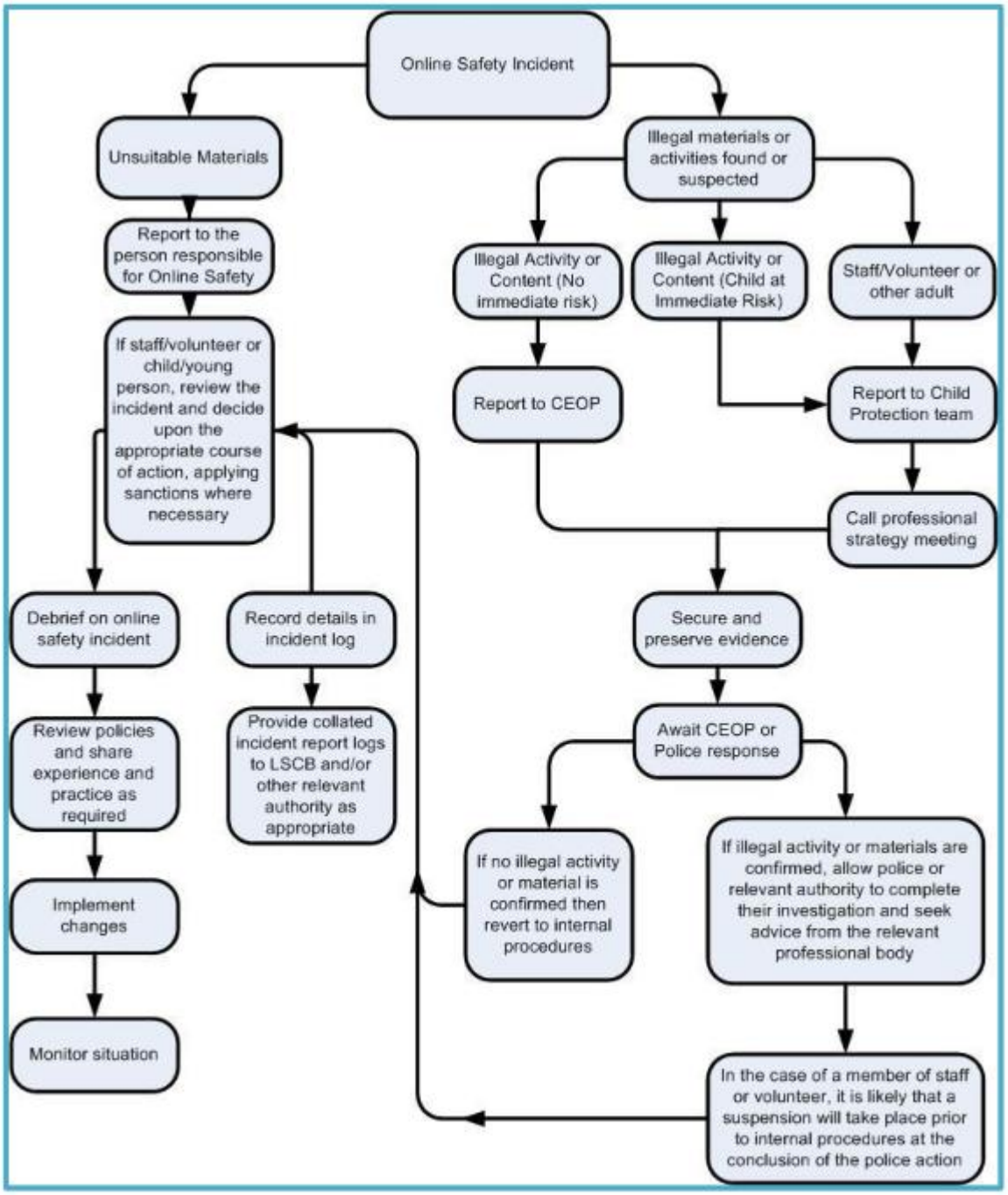
		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse 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	
	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 / 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 (see “User Actions” above).

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 and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school / 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 / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

School Actions & Sanctions

It is more likely that the school / 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 / Sanctions**

Incidents:	Refer to class teacher	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
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X					
Unauthorised use of non-educational sites during lessons	X						X	
Unauthorised use of mobile phone / digital camera / other mobile device	X	X			X			
Unauthorised use of social media / messaging apps / personal email					X		X	
Unauthorised downloading or uploading of files	X			X				
Allowing others to access school network by sharing username and passwords	X						X	
Attempting to access or accessing the school network, using another student's / pupil's account	X						X	
Attempting to access or accessing the school network, using the account of a member of staff		X			X			X
Corrupting or destroying the data of other users		X		X				X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X		X			X
Continued infringements of the above, following previous warnings or sanctions		X		X				X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X		X				X
Using proxy sites or other means to subvert the school's / school's filtering system					X		X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X	X	X		X	X
Deliberately accessing or trying to access offensive or pornographic material		X	X		X			X
Receipt or transmission of material that infringes the copyright of another person or infringes the GDPR (2018)		X						X

Staff **Actions / Sanctions**

Incidents:	Refer to Chair of Governors if incident relates to Headteacher	Refer to line manager	Refer to Headteacher	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 (see list in earlier section on unsuitable / inappropriate activities).	X	X	X		X				X
Inappropriate personal use of the internet / social media / personal email	X	X	X				X		
Unauthorised downloading or uploading of files	X	X				X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X				X	X		
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	X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X		X			X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X		X	X	X			X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X		X	X					X
Actions which could compromise the staff member's professional standing	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	
Accidentally accessing offensive or pornographic material and failing to report the incident	X		X	X					
Deliberately accessing or trying to access offensive or pornographic material	X		X		X			X	X
Breaching copyright or licensing regulations	X		X						X
Continued infringements of the above, following previous warnings or sanctions	X		X					X	X