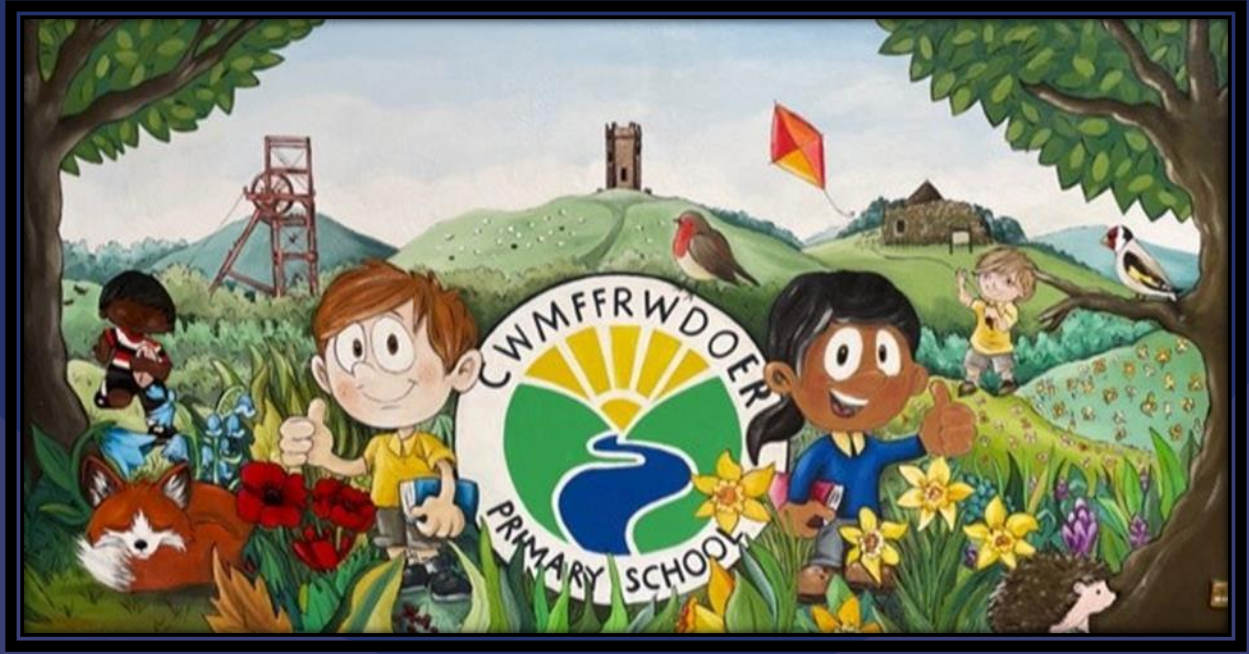


360 safe Cymru

Online Safety Policy



Contents

| | |
|---|------------------------------|
| Introduction | 3 |
| Guidance notes | Error! Bookmark not defined. |
| Online Safety Policy | 4 |
| Scope of the Online Safety Policy | 5 |
| Policy development, monitoring and review | 5 |
| Schedule for development, monitoring and review | 6 |
| Process for monitoring the impact of the Online Safety Policy | 6 |
| Policy and leadership | 7 |
| Responsibilities | 7 |
| Online Safety Group | 14 |
| Professional Standards | 15 |
| Policy | 16 |
| Online Safety Policy | 16 |
| Acceptable use | 17 |
| User actions | 18 |
| Reporting and responding | 21 |
| Responding to Learner Actions | 26 |
| Responding to Staff Actions | 28 |
| Education | 30 |
| Online Safety Education Programme | 30 |
| Contribution of Learners | 32 |
| Staff/volunteers | 33 |
| Governors | 33 |
| Families | 34 |
| Adults and Agencies | 35 |

| | |
|--------------------------------|----|
| Technology..... | 36 |
| Filtering..... | 36 |
| Monitoring..... | 38 |
| Technical Security | 39 |
| Devices | 41 |
| Social media | 43 |
| Digital and video images | 45 |
| Online safety messaging | 46 |
| Data Security | 47 |
| Cyber Security..... | 49 |
| Outcomes..... | 51 |

Introduction

The Education Act 2002 and the Children Act 1989 require Local Authorities and schools to ensure children and young people are safe from harm. Schools are subject to an increased level of scrutiny of their online safety practices by Estyn Inspectors during inspections, while the Counter Terrorism and Securities Act 2015 requires schools to ensure that children and young people are safe from terrorist and extremist material on the internet.

[Keeping Learners Safe](#) (April 2022) states:

7.16 The ability of educational establishments to recognise, respond to and resolve online safety issues should be verified by inspections from Estyn and the local authority.

[Enhancing digital resilience in education: An action plan to protect children and young people online](#) (November 2022) states:

We, the Welsh Government, on behalf of Welsh Ministers, aim to help protect children and young people from illegal, harmful and false content on the internet and to promote safe, responsible and considerate behaviour online.

With so many aspects of our lives now entwined with using technology in an online world, supporting our children and young people to be digitally resilient is fundamental.

Keeping children and young people safe online is of critical importance and firmly a safeguarding matter in the twenty first century. We are committed to nurturing and promoting the safe and positive use of technology to children and young people by building a strong architecture around the child where professionals are skilled and families are aware of how to support children in their online lives. We seek to foster a protective environment for our children and young people by supporting families, practitioners, governors and other professionals creating a culture where keeping children safe online is everyone's business.

The Curriculum for Wales aims to provide all our learners with high-level digital skills, to ensure our young people are digitally competent and resilient and evolve into enterprising, creative and critical thinkers.

Cwmffrwdor Primary School

Online Safety Policy

This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal devices on the school site (where allowed).

Date created: [20/05/24]

Next review date: [20/05/25]

Next review date: [20/06/26]

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Cwmffrwdoer Primary School to safeguard members of our school community online in accordance with principles of open government and with the law. Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced as outlined in the attached 'Legislation' Appendix.

This Online Safety Policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal devices on the school site (where allowed).

Cwmffrwdoer Primary 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 online safety behaviour that take place out of school.

Policy development, monitoring and review

This Online Safety Policy has been developed by the *stakeholders of Cwmffrwdoer Primary school*, made up of:

- *headteacher/senior leaders*
- *online safety lead*
- *staff – including teachers/education practitioners/support staff/technical staff*
- *governors*
- *parents and carers*
- *community users*

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for development, monitoring and review

| | |
|--|--|
| This Online Safety Policy was approved by the <i>school governing body</i> on: | <i>22nd May 2024</i> |
| The implementation of this Online Safety Policy will be monitored by: | <i>Mr Callum Phillips (Digital Lead)</i> <i>Mrs Sarah Roque (Headteacher)</i> |
| Monitoring will take place at regular intervals: | <i>At least once a year.</i> |
| The <i>governing body</i> will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals: | <i>At least once a year.</i> |
| The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be: | <i>To be reviewed annually.</i> |
| Should serious online safety incidents take place, the following external persons/agencies should be informed: | <i>Mrs Sarah Roque (Headteacher)</i> |

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- *logs of reported incidents*
- *monitoring logs of internet activity (including sites visited)*
- *internal monitoring data for network activity*
- *surveys/questionnaires of:*
 - *learners*
 - *parents and carers*
 - *staff.*

Policy and leadership

Responsibilities

In order to ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals¹ and groups within the school.

Headteacher and senior leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to an appropriate member of the senior leadership team.
- 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 online safety allegation being made against a member of staff².
- The headteacher/senior leaders are responsible for ensuring that all staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The headteacher/senior leaders will receive regular monitoring reports from the Online Safety Lead.

¹ In a small school some of the roles described may be combined, though it is important to ensure that there is sufficient 'separation of responsibility' should this be the case.

² See flow chart on dealing with online safety incidents in '[Responding to incidents of misuse](#)' and relevant local authority HR/other relevant body disciplinary procedures.

Governors

[Keeping Learners Safe](#) states:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the Welsh Government and UKCIS document [Five key questions for governing bodies to help challenge their school to effectively safeguard their learners](#). This will be carried out by the Online Safety Committee whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Governor³

to include:

- regular meetings with the Online Safety Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- reporting to relevant *governors group/meeting*
- *membership of the school Online Safety Group*
- *occasional review of the filtering change control logs and the monitoring of filtering logs (where possible)*

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

³ It is suggested that the role may be combined with that of the designated governor for safeguarding. In other settings this may be the management committee person for child protection

Online Safety Lead

The online safety lead will:

- lead the Online Safety Group
- work closely with the Designated Safeguarding Person (DSP), where these roles are not combined
- take responsibility for online safety issues, being aware of the potential for serious child protection concerns
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned and embedded
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- receive reports of online safety incidents⁴ and create a log of incidents to inform future online safety developments
- provide (or identify sources of) training and advice for staff/ governors/ parents/ carers/ learners
- liaise with (school/local authority) technical staff, pastoral staff and support staff (as relevant)
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs
- report regularly to headteacher/senior leadership team.
- liaises with the local authority/relevant body.

⁴ The school will need to decide how these incidents will be dealt with and whether the investigation/action will be the responsibility of the online safety lead or another member of staff, e.g. headteacher/senior leader/Designated Safeguarding Person/class teacher/head of year, etc.

Designated Safeguarding Person (DSP)

Keeping Learners Safe states:

2.14. "The headteacher/principal must appoint the appropriate number of DSPs and deputy DSPs for their education setting and should ensure the DSP:

- is given sufficient time and resources to carry out the role effectively, which should be explicitly defined in the postholder's job description
- has access to the required levels of training and support to undertake the role, including online safety training
- has time to attend and provide reports and advice to case conferences and other inter-agency meetings as required
- has the appropriate IT equipment to carry out the role effectively."

The Designated Safeguarding Person should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

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

Curriculum Leads

The Keeping Learners Safe safeguarding audit tool suggests:

"The curriculum should support existing policy within the education setting on important issues and provide sufficient information on managing risk, e.g. in: sex and relationships; drug, alcohol and tobacco education; accident prevention; anti-bullying; online safety; extremism and radicalisation."

Curriculum Leads will work with the online safety lead to develop a planned and coordinated online safety education programme. This will be provided through

- a discrete programme (*Common Sense Media Resources*)
- the Digital Competence Framework
- relationships and sexuality education
- Health and Wellbeing area of learning and experience
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood and signed the staff acceptable use agreement (AUA), and that this is reviewed regularly
- they immediately report any suspected misuse or problem.
- for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners, parents and carers should be on a professional level *and only carried out using official school systems and devices*
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and 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 learners should be guided to sites that are checked as suitable for their use *and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- they have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Network manager/technical staff (TCBC and SRS)

The network manager/technical staff (or local authority/managed service provider) is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy in order to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the local authority, Welsh government via the [Education Digital Standards](#) or other relevant body
- users may only access the networks and devices through a properly enforced password protection policy
- they keep up-to-date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of the technical and communications systems is regularly monitored in order that any misuse/attempted misuse can be reported for investigation and action
- *The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.*
- *Monitoring software/systems are implemented and updated as agreed in school or education technology support partner policies*

Learners

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and this is reviewed annually.
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology
- should avoid plagiarism and uphold copyright regulations
- will be expected to know and follow school Online Safety Policy
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and carers

Enhancing digital resilience in education: An action plan to protect children and young people online (November 2022) states:

"We are committed to nurturing and promoting the safe and positive use of technology to children and young people by building a strong architecture around the child where professionals are skilled and families are aware of how to support children in their online lives. We seek to foster a protective environment for our children and young people by supporting families, practitioners, governors and other professionals creating a culture where keeping children safe online is everyone's business."

The school will take every opportunity to help parents and carers understand these issues through:

- providing them with a copy of the learners' acceptable use agreement.
- publish information about appropriate use of social media relating to posts concerning the school
- seeking their permissions concerning digital images, cloud services etc
- *providing opportunities for parents and carers to improve their understanding of online safety through parents'/carers' evenings, newsletters, letters, website, Hwb, learning platform and information about national/local online safety campaigns and literature.*
Regular Digital Coffee Morning's with an online safety focus.

Parents and carers will be encouraged to support the school in:

- *reinforcing the online safety messages provided to learners in school*

Community users

Community users who access school systems/website/Hwb/learning platforms as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems.

The school encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other schools and the community.

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the Online Safety Policy including the impact of initiatives.

The Online Safety Group has the following members:

- online safety lead
- Designated Safeguarding Person
- senior leaders
- online safety governor
- technical staff
- teacher and support staff members
- learners
- parents/carers
- community representatives

Members of the Online Safety Group will assist the Online Safety Lead with:

- the production/review/monitoring of the school Online Safety Policy/documents
- the production/review/monitoring of the school web filtering policy and requests for filtering changes
- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage of the Digital Competence Framework
- reviewing network/web filtering/monitoring/incident logs, where possible
- encouraging the contribution of learners to staff awareness, recent trends and the school online safety provision
- consulting stakeholders – including staff/parents/carers about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe Cymru self-review tool.

Professional Standards

There is an expectation that national [professional standards](#) will be applied to online safety as in other aspects of school life i.e.

- there is a consistent emphasis on the central importance of literacy, numeracy, digital competence and digital resilience. Learners will be supported in gaining skills across all areas of learning and every opportunity will be taken to extend learners' skills and competence
- there is a willingness to develop and apply new techniques to suit the purposes of intended learning in a structured and considered approach and to learn from the experience.
- practitioners are able to reflect on their practice, individually and collectively, against nationally agreed standards of effective practice and affirm and celebrate their successes
- policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

Policy

Online Safety Policy

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they can use digital technologies responsibly, protecting themselves and the school and how they can use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through normal communication channels
- is published on the school website.

Acceptable use

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

Acceptable use agreements

An Acceptable Use Agreement is a document that outlines a school's expectations on the responsible use of technology by its users.

The Online Safety Policy and appendices define acceptable use at the school. Within the appendices there are acceptable use agreements for:

- learners – differentiated by age. Learners will be introduced to the acceptable use rules at induction, the start of each school year and regularly re-enforced during lessons, assemblies and by posters/splash screens around the school. *Digital Leaders are encouraged to suggest child friendly versions of the rules.*
- staff /volunteer AUAs will be agreed and signed by staff and volunteers
- parent/carers AUAs inform them of the expectations of acceptable use for their children and seek permissions for digital images, the use of cloud systems etc.
- community users that access school digital technology systems will be required to sign an AUA.

The acceptable use agreements will be communicated/re-enforced through:

- student handbook
- staff induction and handbook
- Signage
- posters/notices around where technology is used
- communication with parents/carers
- built into education sessions
- school website
- peer support.

| User actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|--|---|------------|-----------------------------|--------------------------------|--------------|--------------------------|
| Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: | <p>Any illegal activity for example:</p> <ul style="list-style-type: none"> • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering <p><u>N.B. Schools should refer to guidance about dealing with self-generated nude and semi-nude images (sometimes referred to as 'sexting') - Sharing nudes and semi-nudes: Responding to incidents and safeguarding children and young people.</u></p> | | | | | X |
| Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990) | <ul style="list-style-type: none"> • Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) | | | | | X |

| User actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|------------|-----------------------------|--------------------------------|--------------|--------------------------|
| | N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways – read more about this: NCA Cyber Choices Programme | | | | | |
| Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies: | Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs) | | | | X | X |
| | Promotion of any kind of discrimination | | | | X | 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 | X |
| | Infringing copyright | | | | X | |
| | Unfair usage (downloading/uploading large files that hinders others in their use of the internet) | | | X | X | |
| | Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute | | | | X | |

| <p>Consideration should be given for the following activities when undertaken for non-educational purposes:</p> <p>Schools may wish to add further activities to this list.</p> | Staff and other adults | | | | Learners | | | |
|---|------------------------|---------|--------------------------|----------------------------|-------------|---------|--------------------------|---|
| | Not allowed | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission/awareness |
| Online gaming | | | X | | | | | X |
| Online shopping/commerce | | | | X | X | | | |
| File sharing | | X | | | | | X | |
| Social media | | | X | | X | | | |
| Messaging/chat | | | X | | | | | X |
| Entertainment streaming e.g. Netflix, Disney+ | | | X | | X | | | |
| Use of video broadcasting, e.g. YouTube, Twitch, TikTok | | | X | | X | | | |
| Mobile phones may be brought to school | | X | | | | | | X |
| Use of mobile phones for learning at school | X | | | | X | | | |
| Use of mobile phones in social time at school | | | X | | X | | | |
| Taking photos on mobile phones/cameras | X | | | | X | | | |
| Use of other personal devices, e.g. tablets, gaming devices | | | X | | X | | | |

| | | | | | | | | |
|---|---|--|---|--|---|--|--|--|
| Use of personal email in school, or on school network/wi-fi | | | X | | X | | | |
| Use of school email for personal emails | X | | | | X | | | |

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

- when communicating in a professional capacity, staff should ensure that the communication tools they use are officially sanctioned by the school
- any digital communication between staff and learners or parents/carers (email, social media, learning platform, etc.) must be professional in tone and content.
Personal email addresses, text messaging or social media must not be used for these communications.
- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- users should immediately report to a 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
- *relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school email addresses should be used to identify members of staff and learners.*

Reporting and responding

The school has in place procedures for identifying and reporting cases, or suspected cases, of online safeguarding issues/incidents and understands that because of our day-to-day contact with children our staff are well placed to observe the outward signs of these issues.

We ensure that every member of staff and every governor knows that they have an individual responsibility for reporting and that they are aware of the need to be alert to signs of abuse and neglect, and know how to respond to a learner who may disclose such issues.

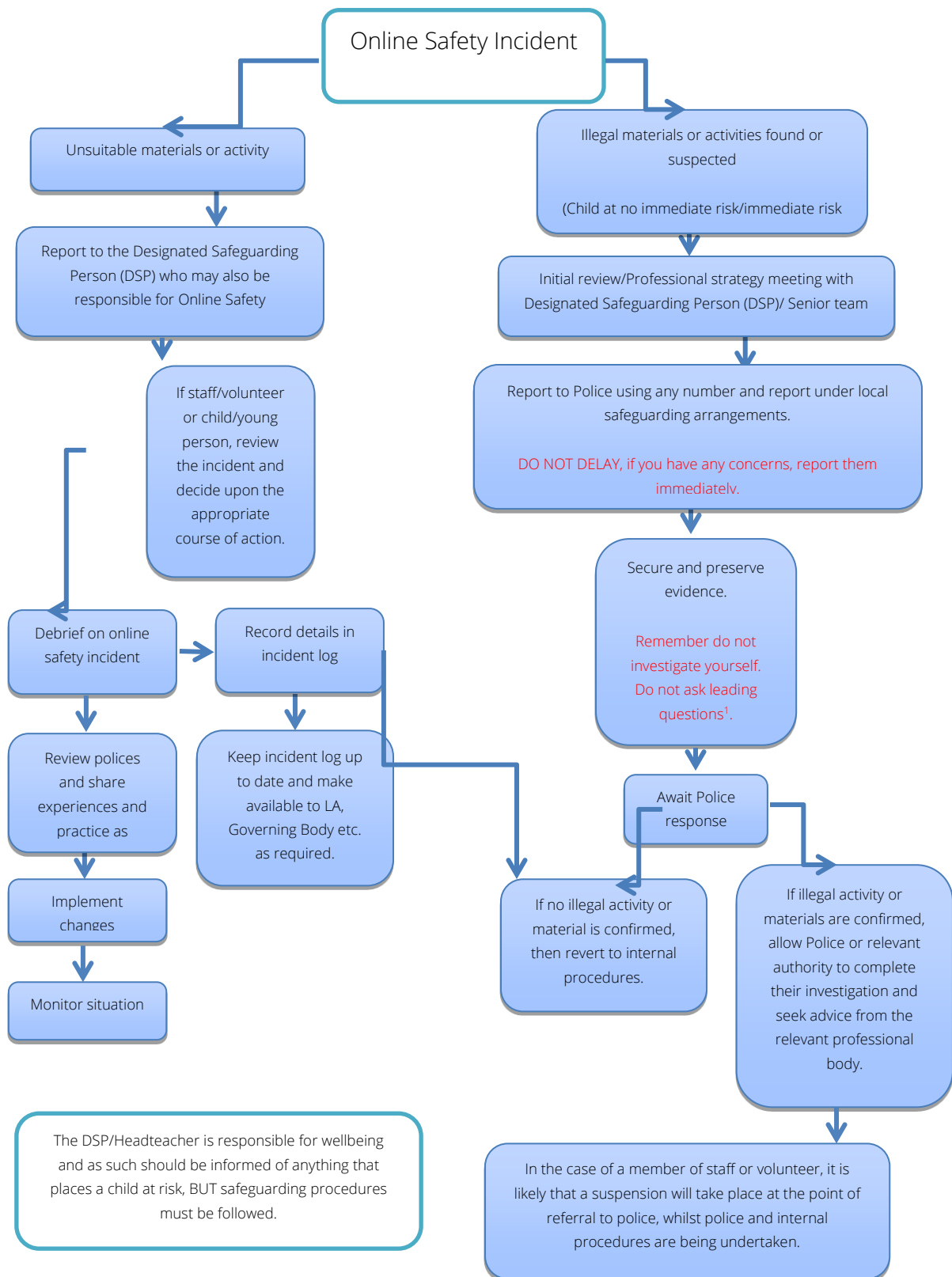
We also understand that reporting systems do not always respond to the needs of learners and that we need to identify issues and intervene early to better protect learners. .

The school will take all reasonable precautions to ensure online safety for all school users, but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies
- all members of the school community will be made aware of the need to immediately report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Person, Online Safety Lead and other responsible staff have appropriate skills and training to deal with the various risks related to online safety
- if there is any suspicion that the incident involves child abuse images, any other illegal activity or the potential for serious harm, the incident must be escalated through the normal school safeguarding procedures and the police informed. In these circumstances any device involved should be isolated to support a potential police investigation. In addition to child abuse images such incidents 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
 - promotion of terrorism or extremism
 - other criminal conduct, activity or materials.
- any concern about staff misuse will be reported immediately to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority
- as long as there is no suspected illegal activity, devices may be checked using the following procedures:
 - one or more senior members of staff should be 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 learners and if necessary can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). 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 above**).
- 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 (as relevant)
 - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g. peer support for those who are reporting or are affected by an online safety incident
- incidents should be logged
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; [Professionals Online Safety Helpline](#); [Reporting Harmful Content](#); [CEOP](#); [Keeping safe online](#) on Hwb
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions
- learning from the incident (or pattern of incidents) will be provided to:
 - *the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with*
 - *staff, through regular briefings*
 - *learners, through assemblies/lessons*
 - *parents/carers, through newsletters, school social media, website*
 - *governors, through regular safeguarding updates*
 - *local authority/external agencies, as relevant*

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.



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:

Responding to Learner Actions

| Incidents | Refer to class teacher/tutor | Refer to Head of Department / Principal Teacher / Deputy Head | Refer to Headteacher | Refer to Police/Social Work | Refer to local authority technical support for advice/action | Inform parents/carers | Remove device/ network/internet access | Issue a warning | Further sanction, in line with behaviour policy |
|--|------------------------------|---|----------------------|-----------------------------|--|-----------------------|--|-----------------|---|
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities). | | X | X | X | X | X | | | |
| Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords | | 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 | | | |
| Unauthorised downloading or uploading of files or use of file sharing. | | 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 | 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 | | | | |
| Unauthorised use of digital devices (including taking images) | | | X | X | | | | | |
| Unauthorised use of online services | | | X | X | | | | | |
| Actions which could bring the school into disrepute or breach the integrity or the ethos of the school. | | | X | X | | X | | | |
| Continued infringements of the above, following previous warnings or sanctions. | | | | X | X | X | X | | X |

Responding to Staff Actions

| Incidents | Refer to line manager | Refer to Headteacher/ Principal | Refer to local authority/MAT/HR | Refer to Police | Refer to LA / Technical Support Staff for action re filtering, etc. | Issue a 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 | | | | |
| Deliberate actions to breach data protection or network security rules. | | X | X | | X | | | |
| Deliberately accessing or trying to access offensive or pornographic material. | | X | 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 | X |
| Using proxy sites or other means to subvert the school's filtering system. | | X | X | | X | | | |
| Unauthorised downloading or uploading of files or file sharing. | | X | X | | X | | | |
| Breaching copyright or licensing regulations. | | 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 | | |

| | | | | | | | | |
|---|--|---|---|---|---|---|---|---|
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature. | | X | X | X | X | X | | |
| Using personal email/social networking/messaging to carry out digital communications with learners and parents/carers | | X | X | X | X | X | X | X |
| Inappropriate personal use of the digital technologies e.g. social media / personal email. | | X | X | | | X | | |
| Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner. | | X | X | | X | | | |
| Actions which could compromise the staff member's professional standing. | | X | | | | X | | |
| Actions which could bring the school into disrepute or breach the integrity or the ethos of the school. | | X | X | | | X | | |
| Failing to report incidents whether caused by deliberate or accidental actions. | | X | X | | | X | X | |
| Continued infringements of the above, following previous warnings or sanctions. | | X | X | X | X | X | X | X |

Education

Online Safety Education Programme

Enhancing digital resilience in education: An action plan to protect children and young people online states:

“With so many aspects of our lives now entwined with using technology in an online world, supporting our children and young people to be digitally resilient is fundamental. Digital resilience encapsulates the need to develop knowledge, skills and strategies in order for children and young people to:

- manage their online experience safely and responsibly while protecting their digital identity
- identify and mitigate risks to stay safe from harm online
- understand the importance of using reliable sources and employing critical thinking skills to identify misinformation
- seek help when they need it
- learn from their experiences and recover when things go wrong
- thrive and benefit from the opportunities the internet offers.”

“Building digital resilience within our children and young people prepares them to become well-rounded and balanced citizens that recognise the impact of their actions. Ensuring our children and young people use technology responsibly to foster a culture where mental and physical health is not adversely affected by the internet is crucial.

Supporting the social and cultural development of our children and young people, including promoting values such as tolerance and respect for others in all environments, is another overarching objective, which we set out to achieve through our online safety education activities.”

Guidance for education settings on peer sexual abuse, exploitation and harmful sexual behaviour states:

“Young people increasingly experience abuse and exploitation online and/or digitally. This will be more difficult for education settings to identify, as some of it is likely to

occur outside schools and colleges. However, it is important to consider the impact of this on young people's offline lives."

While regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the school's safeguarding provision. Learners need the help and support of the school to recognise and avoid online safety risks and develop their resilience.

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

- a planned online safety curriculum across all year groups and a range of subjects, (e.g. DCF/PSE/RSE/Health and Well-being) and topic areas and should be regularly revisited
- key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language. Learners considered to be at increased risk online (e.g. children in care, ALN learners, learners experiencing loss or trauma or mental health issues) are provided with targeted or differentiated online safety education
- learners should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- learners should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- *learners should be helped to understand the need for the learner 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 learners 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 learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit*
- *it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technical staff (or other nominated 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*
- *the online safety education programme will be regularly audited and evaluated to ensure the quality of learning and outcomes.*

Contribution of Learners

[Keeping Learners Safe](#) states:

“How safe do learners feel? The United Nations Convention on the Rights of the Child (UNCRC) sets out that children have a right to be safe and protected from harm, and have the right to express their opinions and participate in decision-making. In accordance with the UNCRC, the best way to understand how safe an education setting feels to learners is to ask them and observe how they and staff interact.”

The school acknowledges, learns from and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- *mechanisms to canvass learner feedback and opinion.*
- *appointment of digital leaders and other pupil voice groups*
- *the Online Safety Group has learner representation*
- *learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns*
- *learners designing/updating acceptable use agreements*
- *contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.*

Staff/volunteers

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

- a planned programme of formal online safety, cyber security and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly. *It is expected that some staff will identify online safety as a training need within the performance management process*
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours
- *the Online Safety Lead and Designated Safeguarding Person (or other nominated person) will receive regular updates through attendance at external training events, (e.g. Hwb Keeping safe online training events, from the Regional Consortium/SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations*
- *this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days*
- *the Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.*

Governors

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

- Hwb training – [Online safety for governors](#)
- attendance at training provided by the local authority or other relevant organisation (e.g. SWGfL)
- participation in school training/information sessions for staff or parents, e.g. Digital Coffee Morning

A higher level of training will be made available to (at least) the Online Safety Governor.

Schools should consider providing all governors with a Hwb account in order to use the secure tools and services available e.g. Microsoft Outlook, Teams etc as well as appropriate application training. This would negate the need for governors to use personal email accounts, thereby reducing the risk to data.

Families

Enhancing digital resilience in education: An action plan to protect children and young people online states:

“Building digital resilience in our children and young people also depends on the resilience of our families and communities. We are committed to nurturing and promoting the safe and positive use of technology to children and young people by building a strong architecture around the child where professionals are skilled and families are aware of how to support children in their online lives. We seek to foster a protective environment for our children and young people by supporting families, practitioners, governors and other professionals creating a culture where keeping children safe online is everyone’s business.”

Many parents and carers have only a limited understanding of online 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 online 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 seek to provide information and awareness to parents and carers through:

- *regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes*
- *regular opportunities for engagement with parents/carers on online safety issues through awareness workshops/parent/carer evenings etc*
- *the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.*
- *letters, newsletters, website, learning platform, Hwb*
- *high profile events/campaigns e.g. [Safer Internet Day](#)*

- reference to the relevant web sites/publications, e.g. Hwb [Keeping safe online](#), [The UK Safer Internet Centre](#), [Childnet International](#)
- *Sharing good practice with other schools in clusters and or the local authority*

Adults and Agencies

The [Enhancing digital resilience in education: An action plan to protect children and young people online](#) draws upon the self-review information schools in Wales record in the 360 safe Cymru tool. This data highlights that schools showing the strongest performance, amongst other indicators,

'ensure that parents and carers receive these important online safety messages, often through the learners themselves sharing the messages learned in school. The school will also share their good practice with the wider community and other schools and will make use of the valuable community resources available to them from agencies such as the police'.

Drawing on this intelligence, the school will provide opportunities for local community groups and members of the wider community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- providing family learning courses in use of new digital technologies and online safety
- online safety messages targeted towards families and relatives.
- the school will provide online safety information via their learning platform, website, and social media for the wider community

The school recognises the support and advice that may be provided by external groups and agencies and values their contribution to school programmes and events.

The school is committed to sharing its good practice with other schools and education settings.

Technology

Cwmffrwdor Primary School has a managed ICT service provided by an outside contractor (SRS), it is the responsibility of the school to ensure that the managed service provider carries out all the online safety and security measures that would otherwise be the responsibility of the school. It is also important that the managed service provider is fully aware of the school Online Safety Policy and acceptable use agreements and the school has a Data Processing Agreement in place with them.

The school is responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures that are in place on a regular basis and explain that everyone is responsible for online safety and data protection..

Filtering

Keeping Learners Safe states:

7.7. "It is critical that web-filtering standards are fit for purpose for twenty-first century learning and teaching, allowing the access schools require while still safeguarding children and young people. Governing bodies should ensure appropriate filters and appropriate monitoring systems are in place and refer to web filtering standards as part of the Education Digital Standards for schools in Wales. The standards seek to support schools to provide a safe, responsible and supportive environment to learn in, and prevent access to inappropriate or harmful content.

- the school filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents and behaviours

- the school manages access to content across its systems for all users. The filtering provided meets the standards defined in the Welsh Government [Education Digital Standards - Web filtering](#) and the UK Safer Internet Centre.
- internet access is filtered for all users
- illegal content (e.g. child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content and this is acted upon in a timely manner by the Designated Safeguarding Person whilst adhering to the Wales Safeguarding Procedures
- there is a clear process in place to deal with requests for filtering changes
- the school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users: staff/learners, etc.)
- younger learners will use child friendly/age appropriate search engines e.g. Google safe search, [SWGfL Swiggle](#)
- there is an appropriate and balanced approach to providing access to online content according to role and/or need
- filtering logs are reviewed frequently and alert the school to breaches of the filtering policy, which are then acted upon.
- *Devices that are provided by the school have school-based filtering applied irrespective of their location.*
- *where personal mobile devices are permitted for use, there is clear separation between the school network filtering and the associated guest network filtering.*
- *the system manages access to content through non-browser services (e.g. apps and other mobile technologies)*

If necessary, the school will seek advice from, and report issues to, the [Report Harmful Content](#) site.

Monitoring

The school monitors network traffic at a local level, follows the UK Safer Internet Centre [Appropriate Monitoring](#) guidance and protects users and school systems through:

- a staff lead who is responsible for managing the monitoring strategy and processes.
- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- monitoring and filtering logs are regularly analysed and breaches are reported to senior leaders
- monitoring enables alerts to be matched to users and devices.
- there is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- management of serious safeguarding alerts is consistent with safeguarding policy and practice.
- *pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.*
- *where possible, school technical staff regularly monitor and record the activity of users on the school technical systems*

Users are made aware, through the acceptable use agreements, that monitoring takes place. Monitoring is carried out by SRS.

Technical Security

The school has a clear technical security policy and systems will be managed in ways that ensure- that the school meets recommended technical requirements:

- system security training is available for all staff users
- there will be regular reviews and audits of the safety and security of school technical systems and of the school's technical support
- servers, wireless systems and cabling are securely located and physical access restricted
- there are rigorous and verified back-up routines, including the keeping of copies off-site or in the cloud and these are resilient by design
- A documented access control model should be in place, clearly defining access rights to school systems and devices. This should be reviewed annually. all users (staff and learners) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Sharing of passwords or username and passwords could lead to an offence under the Computer Misuse Act 1990. Users must immediately report any suspicion or evidence that there has been a breach of security
- all school networks and systems will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password by SRS who will keep an up-to-date record of users and their usernames
- the master account passwords for the school systems are kept in a secure place, e.g. school safe.
- systems are in place for the recovery and resetting of passwords
- **passwords should be long.** *Good practice highlights that password over 12 characters in length are more difficult to crack. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length is more secure than any other special requirements such as uppercase and lowercase letters, number and special characters. Users should be encouraged to avoid using sequential or chronological numbers within their passwords. Passwords/passphrases should be easy to remember, but difficult to guess or crack. See the [Family guide to cybersecurity](#) for more information.*

- Only if necessary, records of learner usernames and passwords for Foundation Phase learners may be kept in an electronic or paper-based form, but they must be securely stored when not required by the user.
- password requirements for learners at Key Stage 2 and above should increase as learners progress through school
- SR 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.
- 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.
- systems and programme software are regularly updated with security patches
- an agreed policy is in place for the provision of temporary access of 'guests', (e.g. trainee teachers, supply teachers, visitors) onto the school systems
- an agreed policy is in place regarding the extent of personal use that users (staff/learners/community users) and their family members are allowed on school devices that may be used out of school
- an agreed device management policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices
- an agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. E.g. encrypted devices.
- systems are in place that prevent the unauthorised sharing of personal data unless safely encrypted or otherwise secured.
- encryption is used for the transfer of sensitive or vulnerable data and on school managed devices
- dual-factor authentication is used for sensitive data or access outside of a trusted network

Devices

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The devices policy should be consistent with and inter-related to other relevant school policies including but not limited to those for safeguarding, behaviour, anti-bullying, acceptable use, and policies around theft or malicious damage. Teaching about the safe and appropriate use of devices should be an integral part of the school's online safety education programme.

In preparing a devices policy the school should consider possible issues and risks. These may include:

- security risks in allowing connections to your school network
- filtering of personal devices
- breakages and insurance
- access to devices for all learners
- avoiding potential classroom distraction
- network connection speeds, types of devices
- charging facilities
- total cost of ownership.

The school acceptable use agreements for staff, learners, parents and carers outline the expectations around the use of devices.

The school allows:

| | School devices | | | Personal devices | | |
|---------------------|---------------------------------|---------------------------------|--------------------------------|------------------|-------------|---------------|
| | School owned for individual use | School owned for multiple users | Authorised device ⁵ | Student owned | Staff owned | Visitor owned |
| Allowed in school | Yes | Yes | Yes | Yes | Yes | Yes |
| Full network access | Yes | Yes | Yes | No | No | No |
| Internet only | | | | No | No | No |
| No network access | | | | Yes | Yes | Yes |

School owned/provided devices:

- *to whom they will be allocated*
- *where, when and how their use is allowed – times/places/in/out of school*
- *if personal use is allowed*
- *levels of access to networks/internet (as above)*
- *management of devices/installation of apps/changing of settings/monitoring*
- *network/broadband capacity*
- *technical support*
- *filtering of devices*
- *access to cloud services*
- *use on trips/events away from school*
- *data protection*
- *taking/storage/use of images*
- *exit processes, what happens to devices/software/apps/stored data if user leaves the school*
- *liability for damage*

⁵ Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

- *staff training.*

Social media

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 learners 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, bully online, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. All staff working at any educational establishment are expected to follow the professional conduct set out by the Education Workforce Council (EWC) and respect learners, their families, colleagues and the school.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published
- providing education/training on social media use including; acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues
- having in place clear reporting guidance, including responsibilities, procedures and sanctions
- risk assessment, including legal risk
- provision of guidance for learners, parents/carers

School staff ensure that:

- no reference is made in social media to learners, parents/carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions are not 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
- they act as positive role models in their use of social media

When official school social media accounts are established there will be:

- a process for approval by senior leaders
- clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under school disciplinary procedures.

Personal use

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, 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
- *the school permits reasonable and appropriate access to private social media sites*

Monitoring of public social media

- As part of active social media engagement, the school will pro-actively monitor the Internet for public postings about the school
- the school will effectively respond to social media comments made by others according to a defined policy or process
- when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

School use of social media for professional purposes will be checked regularly by a senior leader and the Online Safety Group to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the school is unable to resolve support may be sought from the [Professionals Online Safety Helpline](#).

Digital and video images

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

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- should a maintained school or setting choose to use live-streaming or video-conferencing, governing bodies, headteachers and staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the Live-streaming and video-conferencing: safeguarding principles and practice guidance and Keeping Learners Safe para 7.6
- when using digital images, staff should inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites
- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *learners* 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, storage, distribution and publication of those images. Staff/volunteers must be aware of those learners whose images must not be taken/published. 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 learners are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute*
- *learners must not take, use, share, publish or distribute images of others without their permission*
- *photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with good practice guidance on the use of such images*
- *learners' 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 learners are taken for use in school or published on the school website/social media.*
- *parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy*

images will be securely stored on the school network in line with the school retention policy and in accordance with the Data Protection Act 2018

- *learners' work can only be published with the permission of the learner and parents/carers.*

Online safety messaging

The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Social media
- Online newsletters
- Other

The school website is managed/hosted by Mr Callum Phillips. The school ensures that good practice has been observed in the use of online publishing e.g. use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is no risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected and full names are not published.

The school public online publishing provides information about online safety e.g. publishing the schools Online Safety Policy; curating latest advice and guidance; news articles etc, creating an online safety page on the school website.

The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process

Data Security

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school:

- has a Data Protection Policy.
- implements the data protection principles and can demonstrate that it does so
- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed
- has an Information Asset Register (IAR) in place and knows exactly what, where, why and which member of staff has responsibility for managing it
- the IAR lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule' supports this
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- provides staff, parents, volunteers, teenagers and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice
- has procedures in place to deal with the individual rights of the data subject.

- carries out Data Protection Impact Assessments (DPIAs) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
- understands how to share data lawfully and safely with other relevant data controllers.
- has clear and understood policies and routines for the deletion and disposal of data
- reports any relevant breaches to the Information Commissioner within 72 hours of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. To do this it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- as a maintained school, has a Freedom of Information Policy which sets out how it will deal with FOI requests
- provides protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff

When personal data is stored on any mobile device or removable media the:

- data will be encrypted and password protected.
- device will be password protected.
- device will be protected by up to date virus and malware checking software
- data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

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
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school

- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- only use encrypted mobile devices (including USBs) for personal data, particularly when it is about children
- will not transfer any school personal data to personal devices.
- use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

Cyber Security

[Enhancing digital resilience in education: An action plan to protect children and young people online](#) describes cyber security as:

“The term used to describe how both individuals and organisations can reduce the risk of cyber attacks. Cyber security’s main purpose is to ensure the technology we use (devices such as computers, tablets and smartphones) and the services we access online are protected from the risk posed by cyber crime including theft for gain such as ransomware attacks and seeking competitive advantage, or malicious damage intended to disrupt an organisation’s ability to operate effectively. We store large amounts of personal and organisational information on devices and services and preventing unauthorised access to this information is critical.”

- the school has adopted and made use of the relevant Hwb [Network and Data Security Standards](#)
- the school, in partnership with their education technology support partner, has identified the most critical parts of the school’s digital and technology services and sought assurance about their cyber security
- the school, in partnership with their education technology support partner, has an effective backup and restoration plan in place in the event of cyber attacks
- the school’s governance and IT policies reflect the importance of good cyber security

- staff receive training on the common cyber security threats and incidents that schools experience

the school has a business continuity and incident management plan in place that includes IT and these wider services.

Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g. online safety education, awareness and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

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. Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in March 2024. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.

© SWGfL 2024