Rhydypenau Primary School

"Aiming High"

Online Safety Policy

DEVELOPMENT, MONITORING & REVIEW OF THIS POLICY

This Policy will be reviewed regularly, and adapted in line with Local Authority Guidance.

SCHEDULE FOR DEVELOPMENT, MONITORING & REVIEW

This policy was agreed by teachers:	
This policy was agreed and adopted by the Governing Body:	
The implementation of this online safety policy will be monitored by the:	Online Safety Coordinator - C Evered Davies Safe-guarding Officers - N. Hammond, E. Williams, C Evered Davies, C. Sanders. SLT Online Safety Governor
This policy will be reviewed:	Annually, or as required in the light of any significant new developments in the use of technologies, new threats to online safety or incidents that have taken place.
This policy was last reviewed:	Spring Term 2025
This policy is due to be reviewed:	Spring Term 2026
Should serious online safety incidents take place then one or more of the following external persons/agencies should be informed:	Schools ICT Services, Cardiff LEA, Police, Child Exploitation and Online Protection Centre
The Governing Body 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:	Once a term or when necessary
Chair of Governors' Signature	

Headteacher's Signature:	

1. SCOPE OF THE POLICY

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

The Education & Inspections Act 2006 empowers head teachers to such extent as is reasonable, to regulate 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 online safety incidents covered by this policy, which may take place outside of school, but is linked to membership of the school. The Education Act 2011 increased these powers with regard to the searching for and of, electronic devices and the deletion of data. In the case of both Acts, action can only be taken over issues covered by the published Positive Relationships Policy.

The school will deal with such incidents within this policy, and associated 'Positive Relationships' and 'Anti-Bullying' policies, and will inform parents/carers of incidents of inappropriate online safety behaviour that takes place outside of school if such incidents come to their notice.

2. MONITORING THE ONLINE SAFETY POLICY

The school will monitor the impact of this policy using:

- Logs of reported incidents
- Surveys of learners, parents and carers, staff, governors
- Regular reports from the online safety officer.

3. ROLES & RESPONSIBILITIES

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

3.1 GOVERNORS

Governors are responsible for:

- The approval of the online safety policy
- Reviewing the effectiveness of the policy by analysing online safety incidents and other monitoring documents provided monthly.
- Yearly review of the policy.
- All live streaming sessions.

The role of the online safety governor: (see appendix 1 for details)

- regular meetings with the governor responsible for online safety.
- regular monitoring of online safety incident logs.
- reporting to relevant Governors meetings

3.2 HEADTEACHER

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the online safety coordinator.
- The headteacher and the designated child protection officers are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (See section 14, 15: Dealing with online safety incidents, section 14, 15: 'Responding to Incidents of Misuse', and relevant Local Authority HR/other relevant body disciplinary procedures).
- The headteacher and SLT are responsible for ensuring that the online safety coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The headteacher and SLT ensure that there is a system in place to allow for monitoring and support for the Online Safety Coordinator to carry out the internal online safety monitoring role and to provide the team with regular monitoring reports.
- The Headteacher ensures that the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- Is aware of the sites that are approved for use within the school (via Swurl).

- Has responsibility and accountability for all live streaming sessions.

3.3 ONLINE SAFETY COORDINATOR

The online safety coordinator is responsible for:

- Leading the Online safety Committee (see Appendix 2)
- Taking day to day responsibility for online safety issues
- Establishing and reviewing the school online safety policies & documents.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Providing training and advice for staff.
- Liaising with the Local Authority and other relevant bodies.
- Liaising with Schools Information Technology Services.
- Receiving reports of online safety incidents and creating a log of incidents to inform future online safety developments.
- Meeting every term with the governor responsible for online safety to discuss current issues, review incident logs and filtering/change controls.
- Attending relevant governors meetings.
- Reporting regularly to SLT.
- Supporting parents/carers in understanding online safety issues through parents' evenings, meetings, newsletters, letters, websites and information about national or local online safety campaigns.

3.4 TECHNICAL STAFF (SCHOOLS INFORMATION TECHNOLOGY SERVICES)

Technical staff are responsible for ensuring that:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack.
- The school meets required online safety technical requirements and any Local Authority/other relevant body online safety policies/guidance that may apply.
- Users may only access the networks and devices through a properly enforced password protection policy, in which staff passwords are changed regularly and pupils are taught about secure passwords. (See section)
- 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 network/internet/virtual learning environment/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/ online safety coordinator for investigation/action/sanction.
- Software licence logs are accurate and up to date and that any software they upload has the requisite number of licences.
- Internet access is filtered for all users. The broadband/filtering provider filters illegal content by actively employing the Internet Watch Foundation CAIC list.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Ensuring the filtering system is always functioning effectively.
- Using SWURL to list any inappropriate websites, which break through the filter.

3.5 SCHOOL STAFF

Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current RPS Online-safety Policy and school practices.
- They have read and understood the policy and any linked related policies.
- They act as good role models in their use of digital technologies.
- They report any suspected misuse or issues to the relevant person for investigation/action/sanction.
- All digital communications they make are on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and all digital activities.
- Pupils understand and follow the online safety and acceptable use policies.
- They monitor the use of digital equipment and implement current policies with regard to these devices. (Appendix 3)
- They refer to the permissions database before allowing children to undertake online work or before publishing any work/ photos of children. (See Permissions Database)
- They guide pupils to sites checked as suitable for their use and ensure that the processes for dealing with any unsuitable material that is found in Internet searches are followed.
- Children use the appropriate search engines and are not searching without a specific purpose.
- They take care of the equipment they are allocated personally, and for pupil use. They store the equipment in the designated areas and ensure cabling is secure and safe.

- They block inappropriate sites using the SWURL system

3.6 ADMIN STAFF

In addition to the responsibilities outlined in the 'School Staff. section, school admin staff are responsible for:

- The upkeep of the permissions register.
- Giving supply teachers/ visitors login details when they arrive at school.
- Ensuring supply teachers/ visitors sign the acceptable use agreement on arrival at school.
- Changing supply teacher Hwb logins monthly.

3.7 CHILD PROTECTION OFFICERS

The Child Protection Officer are trained in online safety issues and are aware of the potential for serious child protection/safeguarding issues to arise from:

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

3.8 Science & Technology AoLe Team

The online safety group is responsible for ensuring that:

- Reviewing and updating the school online safety policies.
- Mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression.
- Monitoring network/internet/incident logs.
- Consulting stakeholders – including parents/carers and the students/pupils about the online safety provision.
- Monitoring improvement actions identified through the use of the 360 Degree Safe Self Review Tool.
- Supporting parents/carers in understanding online safety issues through parents' evenings, meetings, newsletters, letters, websites and information about national or local online safety campaigns.

3.9 PUPILS

Pupils are responsible for ensuring that:

- they use school digital technology systems in accordance with the Pupil Digital Acceptable Use Policy (Appendix 4)
- they understand the importance of reporting incidents of abuse/ misuse of digital technologies.
- they inform their teacher/ online safety coordinator / online safety digital leaders of any incidents that arise whilst they are using technology - including those involving other children/ adults.
- they understand their parent's wishes regarding publication of work and photographs and that they follow their wishes. (KS2 Pupils)
- they understand that what they learn about online safety applies outside school and realise that, if something they do online relates in any way to school, the school's policy applies to out of school actions.

3.10 PARENTS/CARERS

The school recognises the crucial role that parents/carers play in ensuring their children understand the need to use the Internet/digital devices in an appropriate way.

Parents/ carers are responsible for:

- Supporting the school in promoting good online safety practice.
- Following the school policies related to online safety.
- Working with the school to educate and support pupils when they are involved in, or affected by, incidents regarding online safety.

3.11 COMMUNITY USERS (e.g. Supply Teachers, Visitors etc.)

Community Users who access school systems as part of the wider school provision will be expected to sign the Community User Acceptable Use Policy (Appendix 5) before being provided with access to the school systems.

Supply teachers will be provided with the supply teacher log in by school administration staff.

4 EDUCATION AND TRAINING

4.1 Pupils

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum whenever digital devices are used. The online safety curriculum is broad, relevant and provides progression, with opportunities for creative activities. It is provided in the following ways:

- A planned online safety curriculum is provided and is regularly revisited. This teaching includes:
    - Being critically aware of the materials/content they access online and how to validate the accuracy of the information they find.
    - Acknowledging the source of information they use and respecting copyright when using material accessed on the internet.
    - Being aware of the risks attached to the sharing of personal details.
    - Understanding strategies to deal with inappropriate communications.
    - Understanding how to communicate appropriately when using digital technologies.
    - the difference between personal and professional communications.
    - How to recognise bias and stereotyping.
    - Understanding the way data is stored and manipulated online, their rights and responsibilities involving data use.
    - Understanding the risks associated with the taking, using, sharing, publication and distribution of images.
    - Understanding the risks and benefits of publishing to social media.
- Key online safety messages are reinforced during assemblies and circle time activities.
- Pupils are helped to understand the need for the Pupil Acceptable Use Agreement and the need to adopt safe and responsible use both within and outside school.
- In lessons where Internet use is pre-planned pupils are taught how to find the most suitable sites for their work and which search engines are most suitable for their age group.
- Learners are 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.

4.2 Parents/Carers and the Wider Community

The school provides information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters
- High profile events e.g. Safer Internet Day
- Reference to the relevant websites/publications
- Providing family learning courses in use of new digital technologies, digital literacy and online safety.
- A designated page on the school website.

4.3 Staff and Volunteers

All staff receive online safety training and understand their responsibilities, as outlined in this policy. Training is offered as follows:

- An audit of the online safety training needs of all staff is carried out once a year. Following this audit a planned programme of formal online safety training is made available to all staff. This is regularly updated and reinforced.
- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school Online safety Policy and Acceptable Use Agreements.
- The Online Safety Coordinator receives regular updates through attendance at external training events (e.g. from SWGFL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- The Online Safety Policy and its updates are presented to and discussed by staff in staff/team meetings/INSET days.
- The Online safety Coordinator will provide bespoke advice/guidance/training to individuals as required.

4.4 Governors

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

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

5. TECHNICAL ISSUES

Technical support at Rhydypenau Primary School is managed by School IT Support and is managed in order to effectively and safely meet the school's requirements according to local authority guidance. Major technical issues are managed by them either remotely or when they visit the school.

6. PRIVACY AND THE SCHOOL SYSTEM

All users of the school system are advised that they have no right of privacy for any digital content.

Digital content produced/ stored/ distributed by staff, pupils or governors and stored on any school system may be monitored at any time without prior consent.

7. DATA PROTECTION POLICY

This section is to be read in conjunction with the RPS Data protection and password policies.

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 & secure
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Only transferred to others with adequate protection

The following advice applies to the storage of data by staff other than administration staff.

- Data (which includes photographs of pupils) is stored only in the following places:
    - School server
    - Shared folder on Hwb system (Staff do not store pupil data on their individual drive/ folders/ Hwb onedrive and data is never transferred from a school system to a personal device.)
    - Shared folder on Rhydypenau Google for Education Drive.
    - Portable storage devices are not used to transfer data in RPS
- Emails are sent using the school system address only.
- When sending emails to groups of people who are not staff members, we use the BC address bar in order to prevent email addresses being made public.

- When children leave school their work/ emails will be deleted as part of the SIMS system unless being stored for monitoring purposes. In this instance their work will be retained for only as long as required for the monitoring period.
- When staff leave school they may transfer their username and personal folders to their new institution via Hwb. They should not transfer any pupil data that should have been stored on the shared drive. This data should be deleted.
- Usernames and passwords are private and are not shared by adults. Pupil passwords follow the agreed password policy.
- Data is not transferred on memory sticks or other portable memory devices.
- Staff lock computers when they are not in use (ctr, alt, delete) or by shutting them down.
- Pupils are taught about data issues as part of their regular learning.
- Where staff use their personal devices to view data stored on the school system they must ensure that this must be password protected. These personal devices should be protected in such a way that other users, including family members, do not have access to any secure or sensitive material.
- Where Live streaming/ Video conferencing meetings are recorded they are stored in the Hwb Google for Education Drive in the 'Video Recordings' folder in the (See Video Conferencing Policy).

If there is a breach of data please inform a member of SLT immediately.

8. MOBILE/ PERSONAL DEVICES POLICY

Mobile technology devices may be school/college owned/provided or personally owned and might include smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's/college's wireless network. The device then has access to the wider internet which may include the school/college learning platform and other cloud-based services such as e-mail and data storage.

A range of mobile devices are used by the school to deliver the Curriculum of Wales. All users understand the primary purpose of the mobile/ personal devices in school is educational. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's online safety education programme.

All school equipment remains the property of Cardiff Local Authority and are subject to routine monitoring without prior notice. They must be surrendered immediately upon request by the headteacher, deputy headteacher or member of the SLT.

There is no expectation of privacy for any user and the devices can be monitored at any time. This includes personal devices if they are used on school property or are connected to the school system in any way.

8.1 SCHOOL OWNED TECHNOLOGY

The school currently has a range of devices for use by children and adults in the school. These include ipads, laptops, chrome books, data loggers etc. Although the majority of children have equal access to devices (see equal opps policy) some children may need increased or personalised access.

- Each class teacher has permanent use of a laptop and tablet. Whilst the laptop is for school use only, devices may be used off site. Personal use of these devices is permitted but is restricted to times outside of school teaching time. If a teacher is out of class for any reason they must leave the laptop for use by their cover teacher/ TA.
- There is a bank of Chromebooks available for teaching assistants/ other support staff. These may be used off-site. Personal use of these devices is permitted but is restricted to times outside of school teaching time.
- Year groups have a designated set of chrome books (1 per child in KS2) and tablets that are allocated for their use although, on occasions, year groups may borrow from each other. This must be arranged with the year group ***prior to the lesson taking place.*** This technology is for school use only and must not be removed from the school premises without prior permission. Personal use of these devices is not the norm, although, on occasions, pupils may be allowed to use the devices as part of a

reward system. In this case nothing should be downloaded onto the device and the member of staff giving the reward is responsible for viewing the content and confirming its suitability for use by pupils.

8.2 CONNECTING TO THE SCHOOL NETWORK

Staff laptops connect automatically via the 'curriculum' network. All other school mobile devices connect to the network via the Public network.

Staff personal devices may be connected to the public network but their use must comply with the social media and acceptable use policies. Personal mobile devices may only be used outside of teaching time, unless it is to make work-based calls.

8.3 PERSONALISING EQUIPMENT

Staff Ipads

- Users may download appropriate apps to use with their class, or as part of their wider role by requesting apps through the school's IT support service.
- Staff are not to allow use of the ipad by anyone outside of RPS.

Staff Laptops/ Chrome book

- Staff may download updates to existing apps as required.
- Any new software downloads must be carried out by the school's IT Support Service or agreed by a member of the SLT prior to downloading.
- Staff are not to allow use of the tablet by anyone outside of RPS.
- Users must not attempt to remove any limitations put onto school equipment. (e.g. Jailbreaking, altering operating systems).

8.4 BRING YOUR OWN DEVICES

Staff do not use their own devices on the curriculum network. This excludes the device provided by WG for use by teachers outside school.

RPS does not currently allow pupils to use their own devices in school. This includes any device which can send and receive communications (e.g. phones, smart watches, fit bits etc). Where pupils do need to bring in a mobile device for use before and after school, they are given to the teacher at the beginning of the day and can be collected once school has finished.

8.5 BREAKAGES

Any breakages are reported to the ICT coordinator as soon as possible. On occasion, for example if inappropriate behaviour was involved, it may also need to be reported to the

online safety officer. In the case of deliberate breakages please refer to the acceptable use policy.

9. POLICY FOR THE USE OF DIGITAL & 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 we are aware that staff, parents and carers and learners need to be made aware of the risks associated with publishing digital images on the internet e.g.

- 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.

All staff are responsible for informing and educating users about these risks and how to reduce the likelihood of the potential for harm - In particular the risks attached to publishing their own images on the internet e.g. social networking sites.

9.1 PROCEDURES - SCHOOL STAFF

- Staff and volunteers are allowed to take, download, share, adapt and distribute digital images/videos, which include images of pupils, to support educational aims and in accordance with the principles behind our teaching.
- Those images are only taken on school equipment.
- These images are only taken for the following specific purposes:
    - sharing information with parents/ other staff members within the school systems **inc email, eg for competitions,
    - updating school communications/ web pages/ displays
    - as part of a project or school work
- Images are stored on school systems only and are removed once the pupils have left the school, except when the photographs are being used for monitoring or evidence of provision. In this case the photographs will be removed once the monitoring has taken place.
- When publishing children's images outside of seesaw/ school server/ hwb storage, staff check whether parents have given their permission prior to publication. (In KS2 pupils are expected to withdraw themselves from such photos but the onus is on the staff member to check this.)
- As a general rule individual photographs of pupils are not published, we prefer to use group photos of children.
- We take care when publishing digital images/videos that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- Pupils full names will not be used on any **external publication** in association with photographs, nor will locations be mentioned (unless posting AFTER an activity has taken place).

9.2 PROCEDURES - PARENTS

- Parents/carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases, protection, parents are informed before such events that these images are not to be:
    - published/made publicly available on social networking sites/ websites
    - commented on to include names of children/staff

9.3 PROCEDURES - PUPILS

- Pupils are allowed to take, download, share, adapt and distribute digital images/videos, which include images of pupils, to support educational aims and in accordance with the principles behind our teaching.
- Pupils may publish digital images that include themselves or other children in the school system only. At KS2 pupils may only publish their own, or other childrens images, with permission from the children in the photograph. In Foundation Learning, pupils should be encouraged to ask children before publishing photographs and mistakes discussed as part of their learning.

9.4 USE OF ONLINE DIGITAL IMAGES

- Staff, pupils and volunteers use images downloaded from the Internet to support educational aims. These images are copyright free and fit for purpose.

10. COMMUNICATIONS TECHNOLOGIES POLICY

A wide range of rapidly developing communication technologies has the potential to enhance learning. This includes, but is not restricted to, email, video conferencing, chat facilities, document sharing etc.

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

- Staff and pupils use only the school systems to communicate with others when in school or when working on projects related to school.
- Users must immediately report to the Online coordinator 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. They must also report if they are aware of any such material being received by other pupils or staff members.
- Any digital communication between staff and pupils or parents/carers must be professional in tone and in content. These communications may only take place using the official (monitored) school systems, Seesaw or School-to-Parent text system. Personal email addresses, text messaging or social media must not be used for work related communications.
- All pupils are provided with a school email address for use in school, for school projects or to communicate with other pupils.
- When, as part of their school work, pupils send emails to people outside the school domain they will copy in their class teacher and add the phrase ‘when you reply please can you reply all so that my teacher can see your email too’.
- Pupils are taught about the difference between work and home emails and when it is appropriate to use their school emails.
- Personal information will not be posted on the school website and only official school email addresses should be used to identify members of staff.

11. LIVE STREAMING (See appendix 6)

Teachers use live streaming and video conferencing as part of blended learning, to hold parent/ teacher consultations and for other meetings between professionals. They also use meeting software to allow other educational providers to interact with classes.

The guidance outlined in this policy must be observed alongside local authority guidance.

At Rhydypenau primary school video-conferencing or live-streaming:

- Is conducted on a voluntary basis – staff are not directed to undertake video-conferencing or live-streaming lessons or sessions.
- In accordance with WG guidance all lessons/sessions are carried out via Hwb using Microsoft Teams or Google Meet.
- Practitioners only ever carry out video conferencing or live streaming on a school issued device. Staff never use their own personal equipment under any circumstances.
- Sessions are recorded. (See appendix 6)

11.1 ACCEPTABLE USE OF VIDEO CONFERENCING SOFTWARE BY STAFF MEMBERS.

11.1a CARRYING OUT LIVE LESSONS AWAY FROM THE SCHOOL SETTING

Practitioners ensure:

- That there are two members of staff present for every session that is not being led from the school setting.
- That when they are leading a session that involves specific children the session is recorded.
- Students understand that the lesson is being recorded.
- They set a blurred background for every session that takes place outside the school setting.
- They continue to work in the same professional manner as they would in the classroom.
- Lessons are planned in advance.
- That they check that all pupils have relevant permissions ***prior*** to the meeting.
- They provide sufficient notice to pupils, parents and carers to enable them to attend the session.
- They provide pupils, parents and carers with information about the length of the session and how many pupils will be present.
- Ensure pupils are wearing headphones throughout the session.

- That they are mindful of the need for confidentiality; especially if live-streaming a lesson from a venue where other adults or children are present.
- That they end the session for all participants, ensuring learners are not left alone and unsupervised in a lesson/session the practitioner has left.
- They join the meeting before the session starts.
- They never undertake a video-conferencing lesson where only one practitioner and one learner is present.

Practitioners are conscious that in an online environment remarks are being heard by a number of learners and could be easily misconstrued.

11.1b CARRYING OUT LIVE LESSONS IN THE SCHOOL SETTING

When carrying out live sessions in the school setting the same rules apply as from a home setting with the following exceptions:

If the session is part of 'regular' teaching that a small number of children who are outside the class are joining, there is no need for a second member of staff to join the lesson and the lesson does not need to be recorded. (Appendix 6)

If the session involves specific children and is not part of regular class teaching the session needs to be recorded.

11.2 SAFEGUARDING CONCERNS

If staff have any safeguarding concerns about a child, you should discuss these with the Designated Safeguarding Person (DSP) for the school or setting ensuring your concerns are reported as soon as possible.

If for any reason you cannot contact the Designated Safeguarding Person for your school or setting, contact the local authority Children's Services Team and report your concerns. g. If you think a child or young person is in immediate danger then contact the police on 999.

See RPS safeguarding policy

11.3 LIVE STREAMING INVOLVING EXTERNAL ORGANISATIONS

On occasions practitioners may video-conference or live-stream with external organisations. For instance to deliver a music lesson with a musician/group of musicians. These lessons/sessions should be dealt with using the same safeguarding protocols as any other video-conferencing or live-streaming lesson or session in 11.2a, 11.2b.

In addition the practitioner:

- Sets up and controls the session, inviting the external organisation as a guest participant.
- Establishes expectations and communicates the expectations set out in this guidance to the external provider.
- Should ensure they end the lesson/session for all when the lesson/session is over.
- Ensures the number of staff required present is the same as with any other video-conferencing or live-streamed lesson/session (see above)
- Is fully aware of the content that will be provided by the external organisation.
- Checks all content is appropriate and for any tasks requiring online research, check the suitability of the websites prior to the lesson
- Maintains a central record of all online events alongside a list of attendees.

On some occasions, where the organisation is seen by the school as a 'Trusted' organisation, and where sessions are taking place in school, the following will apply:

- the organisation can set up and lead the session.
- the session will not need to be recorded.

See appendix 6 for the list of trusted organisations.

11.4 ACCEPTABLE USE OF VIDEO CONFERENCING SOFTWARE BY PUPILS

Pupils:

- Must not set a background.
- Must behave as they would in class.
- Must notify the practitioner if anyone else is in the room.

11.3 ACCEPTABLE USE OF VIDEO CONFERENCING SOFTWARE BY PARENTS/ CARERS

We recognise that parents/carers may wish to be present when their child is taking part in video meetings/ lessons.

Parents/ carers:

- Must not make recordings of the meeting.
- Should not be present in a meeting which involves pupils other than their own children.
- Must not publish/ share/ adapt all or any part of the meeting on any platform.

12. SOCIAL MEDIA POLICY

13. PASSWORD AND PERMISSIONS POLICY

All users have clearly defined access rights to school systems and devices and all school networks and systems are protected by secure passwords.

13.1 PERMISSIONS

The two school digital champions have access to the user names and passwords of the whole school. They are required to keep this information secure and to only divulge it when reissuing lost passwords or when asked to provide access by the Headteacher as part of the disciplinary process.

All staff have the right to view and change the user details of pupils in their class.

Governors are currently permissioned to access only the Governor Shared Area of the school systems.

13.2 PUPIL PASSWORDS

- On entering schools pupils will be automatically allocated usernames and passwords for the Hwb system.

- Staff members can keep passwords for pupils in Foundation phase to year 3 in paper form. These passwords should be stored securely. From Year 4 on staff will make decisions about individual pupils and whether they need to store their passwords on paper or look them up on the system as they need them. Year 3 are taught to remember their own password.

- From year 4 onwards pupils who are able to remember their own passwords can have them changed to one that suits them, that they keep private. This will be after they learn about strong passwords, and the password they set must follow the secure password procedures. In year 4 we expect there will be limited numbers of children who have their own passwords, by year 5 it will be most of the class and by year 6 it will be expected of all children (except those with SEN).

- Pupils will be taught about password safety from reception.

13.3 STAFF PASSWORDS

- Staff passwords for logging on to the school server are generated by SITS. They are required to be changed every 3 months. This is an automatic process.
- Passwords for professional sites will be set by the teacher. They change their passwords to ones that they will remember and follow the secure password procedure. (Appendix 7) These do not have to be changed regularly as they:
    - Will never be shared with anyone else, even another member of staff/ family member.
    - Will not be written down.
    - Will follow the secure password procedure.
- In some circumstances staff will need to authenticate their log in using activation methods. The 'Microsoft Authentication App' will provide this level of security. This will only be the case when staff are accessing the user system outside the school premise.

13.4 GOVERNOR PASSWORDS

Governor passwords are issued through the Hwb system. They are permissioned to access only the Governors Shared Area.

13.5 PASSWORDS FOR OTHER USERS

Supply Teachers, Visitors who are working as part of the school will log onto the school system using the supply teacher log in issued by SITS.

13.6 SECURE PASSWORD PROCEDURE

All users (adults and learners) have responsibility for the security of their username and password. must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

14. ACCEPTABLE USE OF TECHNOLOGY - ADULTS

14. 1 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:

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.
- Grooming, incitement, arrangement or facilitation of sexual acts against children contrary to the Sexual Offences Act 2003.
- Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) contrary to the Criminal Justice and Immigration Act 2008.
- Criminally racist material in the UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) contrary to the Public Order Act 1986.
- Pornography.
- Promotion of any kind of discrimination.
- Threatening behaviour, including promotion of physical violence or mental harm.
- 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.
- Using school systems to run a private business.
- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school.
- Infringing copyright.
- Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)
- Creating or propagating computer viruses or other harmful files.
- downloading large files that are not to be used as part of the school role.
- Online gaming – non-educational.
- Online gambling.

The following may be used by staff during non-teaching time but should not conflict with any of the above:

- Use of social media – personal accounts.
- Use of messaging apps – personal accounts.
- Online shopping/commerce.

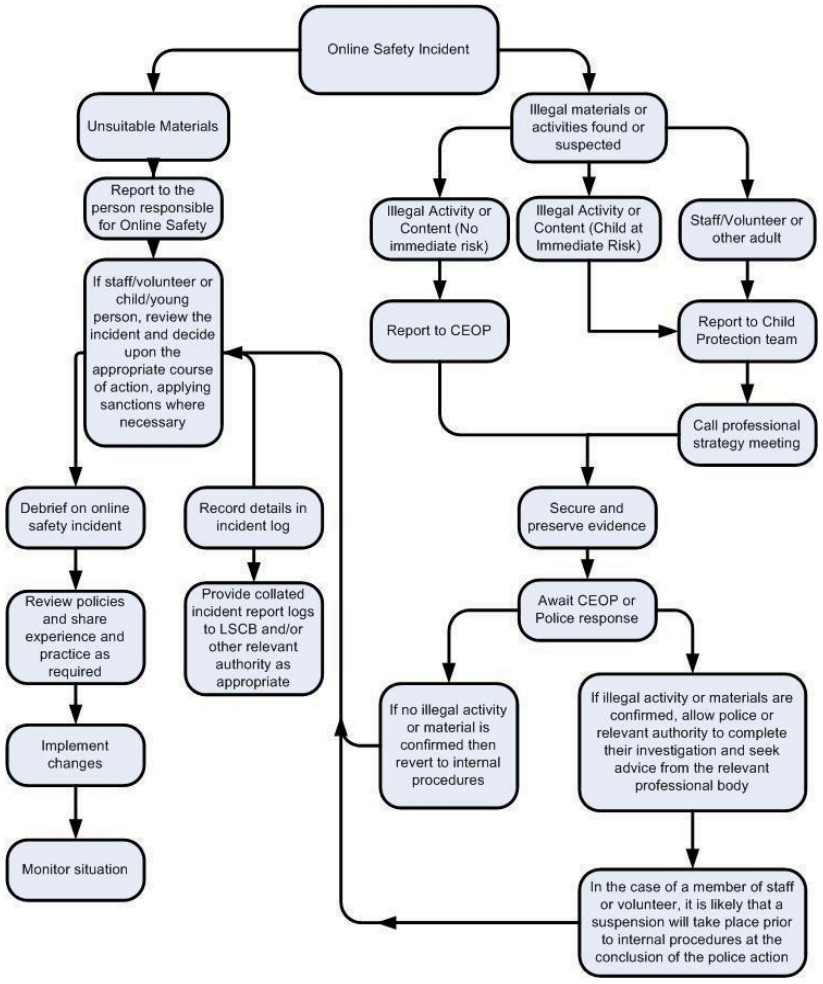
14.2 RESPONDING TO INCIDENTS OF MISUSE - ADULTS

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 Flow Chart for Responding to Online Safety Incidents and report immediately to the police.

This guidance is intended for use when staff need to manage 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).



OTHER INCIDENTS

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

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

- Have more than one senior member of staff involved in this process. 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 further 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 the 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.

14. 3 ACTIONS AND SANCTIONS

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse.
It is essential that 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:

STAFF INCIDENTS	RANGE OF POSSIBLE ACTIONS/SANCTIONS							
	Refer to Online safety Co-ordinator	Refer to Headteacher	Refer to Local Authority/ HR	Refer to Police	Refer to Technical Support Staff for action	Warning	Suspension	Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X				
Inappropriate personal use of the internet/social media/personal email.	X	X				X		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 e.g. holding or transferring data in an insecure manner.	X	X				X		X
Deliberate actions to breach data protection of network security rules.	X	X				X		X

Corrupting or destroying the data of other users or causing deliberate damage to hardware or software.	X	X				X		X
Sending an email/text/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 carry out digital communications with pupils.	X	X				X		X
Actions which could compromise the staff member's professional standing.	X	X				X		X
Actions which could being the school into disrepute or breach the integrity of the ethos of the school.	X	X				X		X
Using proxy sites or other means to subvert the school's filtering system.	X	X	X	X		X		X
Accidentally accessing offensive or pornographic material and failing to report the incident.	X	X				X		X
Deliberately accessing or trying to access offensive or pornographic material.	X	X	X	X		X		X
Breaching copyright or licensing regulations.	X	X				X		X
Continued infringements of the above, following previous warnings or sanctions.	X	X	X			X	X	X

15. ACCEPTABLE USE OF TECHNOLOGY - PUPILS

All pupils sign an acceptable use policy. These policies are geared to the age of the pupils and are developed by the Online Safety Group and the pupil digital leaders. (See appendix 4)

15. 1 RESPONSE TO INAPPROPRIATE USE

Online incidents involving pupils are categorised by ratings - low, medium, high.

Although it is not possible to give definite categories for every possible incident (they are limitless and constantly changing as digital life evolves) we have developed a guide for staff, parents and pupils to understand how incidents will be treated. (Appendix 8)

Staff follow this guide whenever a digital incident takes place. The table is updated to include more details and advice as issues arise and are dealt with.

16. ACCEPTABLE USE OF TECHNOLOGY - Parents

Parents are asked to sign an acceptable use agreement when their child joins the school. The agreement covers the points raised in this policy. (Appendix 9)

Appendix 1 - Online Safety Governor

The online safety governor is:

Name here

They can be contacted via email:

Email address here

Appendix 2 - Monitoring Procedures

Monitoring email communication

Year groups monitor pupil emails once a month. Three pupil accounts from each class are chosen at random and their recent emails are read. An email is then sent to the pupil saying that their account has been monitored and any advice attached to it. Any issues are dealt with in accordance with the acceptable use policy (see section)

Record of monitoring is kept on the Email Monitoring Sheet.

Monitoring data breaches

All systems where pupil data is stored are monitored once a month by staff to record any data breaches. Each year group fills in the Digital Audit Data Breaches sheet - sign and date to show no data breaches.

Rhydypenau Primary School
PUPIL ACCEPTABLE USE POLICY KS2

This is how I stay safe when I use technology in school, and at home for my school work:

- ✓ I think carefully about what I say and do when I communicate with others and have high standards of behaviour when I work online.
- ✓ I am always kind and behave just as I do when I am working with people face to face.
- ✓ I never contact someone outside of our school by email, or using any other online communications, unless my teacher has given me permission and I have copied them into the communication.
- ✓ I am responsible. I only use technology when I have been given permission, and I only use it for my work.
- ✓ I use the sites I have been given - I never go to sites that are not about my school work or that I have not been given permission to use.
- ✓ I try to learn my password, so I can log in by myself. I keep my password a secret.
- ✓ I take care of the school technology equipment and the school network.
- ✓ I don't take photos or record other children or teachers unless they know I am doing it and they have given me their permission.
- ✓ When I am taking part in live streaming sessions involving groups of children I wear headphones.
- ✓ If I bring a device that can receive/ send communications to school I must give it to my teacher at the beginning of the day and collect it at the end. (Phones, watches etc)

I speak to a teacher if:

- ✓ If I see something that upsets me when I am working online.
- ✓ If I see someone else upset by something they see online.
- ✓ I make a mistake and post something I shouldn't or break one of our rules.
- ✓ If I see someone else making a mistake or breaking one of the rules.

Rhydypenau Primary School
Keeping safe when I use technology

When I use technology or go online:

 I am kind and polite.

 I take care of the equipment.

 I only use technology for the things my teacher has told me.

 I try to learn my password.

 I ask people before I take their photo or video them.

 I wear headphones in my online lessons.

I tell my teacher if:

 I am upset about something I see.

 I think someone else is upset by something they see.

 I break one of our rules.

 I see someone else breaking one of our rules.

Appendix 3 - Acceptable Use Community Users

We want to protect you, our pupils and our staff while you are working at Rhydypenau Primary School and keep all our community safe.

Please read and sign this acceptable use document to ensure you stay safe while working at our school.

- I use any online systems responsibly and legally, ensuring that what I present, share or produce will be of educational value and acceptable to the school community.
- While I am at school I use devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users.
- I will ensure that I have viewed any material I intend to use with pupils prior to using it in the school.
- I may use my own laptop or chrome book and sign on to the public network or a teacher will allow me to use the class computer for my work. If I use my own laptop I ensure it is appropriate for school use.
- I do not use any external drives on the school network.
- I understand that my use of school systems, devices and digital communications will be monitored.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will ensure that if I take and/or publish images of others I will only do so with their permission.
- I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will ensure that I have permission to use the original work of others in my own work.

I understand that if I fail to comply with this Acceptable Use Agreement, the school/college has the right to remove my access to school systems.

As the school/college is collecting personal data by issuing this form, it should inform community users about:

who will have access to this form
where this form will be stored
how long this form will be stored for
how this form will be destroyed

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

Name _____Signed _____
Date:

Appendix 4 - Recording Meetings

Procedure for recording live streamed or video conference meetings.

Teams:

a. Record and download the video from the software
b. Upload video to 'Meetings Evidence' folder in staff shared drive on HWB Google for Education.
c. Name with date and details of the meeting. (27/6 Reading lesson MF, JW, SR, TV, PQ)
d. Delete the video from the download folder on the computer.

Google Meets:

Appendix 5 - passwords

Pupil Passwords

Initially, ie when they come into reception, pupil passwords will be set as follows:

Password: pupils initials in capital letters - rps - year they leave school - !
So for Jane Ali who leaves school in 2029 the password will be:
JArps29!

This will enable all pupils to have individual passwords whilst also enabling class teachers/ other adults to be able to log in for them if there are any issues.

Setting secure passwords - advice for staff members

1. Long passwords are harder to break. The best passwords are a series of random words linked together.

   E.g. housepuzzleair

   Pick something you will remember easily without having to right it down.

2. Include at least one capital letter and one symbol/ number
   E.g. h0usepuzzleairhwb!

3. Consider having a stock starter which you end with the first three letters of whatever you are using.
   E.g. housepuzzleairhwb

Appendix 6 - Responding to Pupil Digital Incidents

These are only examples of incidents that occur. If an incident is not listed here, the online safety officer, in conjunction with senior management, will make a decision on where the incident fits. An example will then be added to the list below.

Rating	Examples of incidents	Consequences
Low	All Year Groups ● Producing, publishing, sharing, searching for or viewing 'silly' materials or posts often with childish swear words (bum, willy, bloody), mildly inappropriate pictures or mis-firing attempts to be humorous. ● Inappropriate use of school equipment during school time. (ie, playing games without permissions) FP ● Changing another user's work without their permission. ● Using technology without permission or for something they don't have permission for. In addition all pupils ● Being aware of any of the above and not following acceptable behaviour policy. *Evil Peppa Pig Video* *Coronavirus Message* *Cat song post*	Pupil/s spoken to by teacher and reminded of appropriate behaviour. Teacher to add behaviour to My Concern. Whole year group teaching - What is appropriate? What other children could do? Think before you post. Link to No Outsiders and Values Education. Add
Medium	All pupils ● Producing, publishing, sharing, searching for or viewing materials which could frighten other pupils or cause offence or which, if the child was older, could lead to	Pupil/s are spoken to by the Online Safety Officer who adds the incident to My Concern. Parents are informed of the incident and how it

	criminal charges. These may include stronger swear words (shit, fuck). or, at FP, pictures of body parts. ● Isolated incidents of pettiness/ meanness to one, or more, children. KS2 ● Inappropriate use of technology during school time. (eg using equipment for personal use, to publish to personal pages, taking photos of pupils/adults without their permission) ● Logging on with someone else's username and password without their permission. ● Posting something from someone else's account. ● Changing another user's work without their permission (Y4-5). ● Accidentally accessing offensive or pornographic material and failing to report the incident. (KS2) FP ● Downloading a program/ app onto the school system without permission. Year 6 ● Using Mobile phone in school without permission. All Pupils ● Repeat of low level behaviour. ● Encouraging others to do any of the above.	was dealt with. Some form of punishment - removal of equipment, only supervised use, restorative justice, positive detention (e.g. doing something to improve the school in their own time.) Whole year group teaching - what is appropriate? what other children could do? think before you post. Link to No Outsiders and Values Education.

	• Being aware of, and not following acceptable behaviour policy. *Posting to YouTube channel* *Mumu video*	
High	All Year Groups • Deliberately accessing or trying to access material that is illegal. • Producing, publishing, sharing, searching for, or viewing materials which could cause offence/ upset to individuals or groups of people, or which could inflame a situation between people. This includes (but is not restricted to) racist, homophobic, sexist material or any material that attempts to denigrate a person, or group of people, and goes against our 'No Outsiders' ethos and our Values. • Producing, publishing, sharing, searching for or viewing materials under another person's name or user details. • Cyber bullying or harassment - see Anti-bullying policy • Action which could bring the school into disrepute or breach the integrity of the ethos of the school. • Using proxy sites or other means to subvert the school's filtering system. KS2 • Deliberately downloading a program/ app onto the school system without permission.	If a child is over the age of 10 and a criminal act has been committed the police will need to be informed. Restorative justice parents involved - head/ deputy led, thoroughly investigated, parents involved in the whole process. Some form of punishment - removal of equipment, only supervised use, restorative justice, positive detention ie doing something to improve the school in their own time. whole year group teaching Link to No Outsiders and Values Education. The Child Protection policy will have to be followed if there are any safeguarding issues.

	• Sharing user name or password to someone outside the school to allow them to access the school system. • Attempting to access or accessing the school network, using the account of a member of staff. • Corrupting or destroying the work or data of other users. Year 6 • Changing another user's work without their permission. All Year Groups • Repeat of medium level behaviours. • Encouraging others to do any of the above • Being aware of any of the above behaviours and not following the pupil acceptable behaviour policy.	

Rhydypenau Primary School
Parent and Carer Acceptable Use Policy

Parents/ carers are responsible for:

- Supporting the school in promoting good online safety practice.
- Following the school policies related to online safety.
- Talking with their children about the pupil online safety agreement and encouraging them to follow it.
- Working with the school to educate and support pupils when they are involved in, or affected by, incidents regarding online safety.
- Ensuring they are aware of the permissions they have given for their child and updating them as necessary.
- Acting as good role models when using social media, publishing materials online and communicating with others online.

Taking and use of photographs

Parents/carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases, protection, these images are not to be:

- published/made publicly available online (e.g. social networking sites/ websites)
- commented on to include names of children/staff

Parents should not take photographs of staff or children outside their family without staff or parental permission.

Bringing Communications Devices to School

Many devices now send/ receive communications (e.g. emails, phone calls, texts etc) These include (but are not limited to) mobile phones, watches, music players, glasses. Children can only bring these devices to school with permission from the head teacher and with the understanding they cannot be used in school. They will be handed to the class teacher at the beginning of the day, and collected at the end. If devices such as watches need to be used in school they must be set in such a ways that communication scannot be made from or to them.

Live streamed lessons

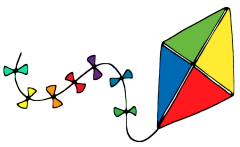
We recognise that parents/carers may wish to be present when their child is taking part in video meetings/ lessons.

Parents/ carers:

- Must not make recordings of the meeting.
- Should not be present in a meeting which involves pupils other than their own children.
- Must not publish/ share/ adapt all or any part of the meeting on any platform.
- Must keep the sessions confidential and must not discuss the content of lessons or pupils responses with people other than the teacher.
- Must ensure that pupils wear headphones when taking part in live streaming sessions involving groups of children.

Social Media

Our aim is to work together with parents and carers to provide the best educational experience for the children in our care.



Parents/carers:

- Should make complaints through official channels not on social networking sites.
- Should not post malicious or fictitious comments on social networking sites about any member of the school or any member of the school community.
- Parents should not post pictures on social media of staff members or children other than their own, without prior permission of the staff member or child's parents/ carers
- Act as role models for their children in their own use of social media.