GAYHURST
SCHOOL

ONLINE SAFETY POLICY

THIS POLICY APPLIES TO ALL MEMBERS OF THE SCHOOL COMMUNITY (INCLUDING STAFF & GOVERNORS, LEARNERS, VOLUNTEERS, PARENTS AND CARERS AND VISITORS) WHO HAVE ACCESS TO AND ARE USERS OF SCHOOL DIGITAL SYSTEMS, BOTH IN AND OUT OF THE SCHOOL.

P073v04
Reviewed: Autumn 2025
Next Review: Autumn 2026
Compiled by: Director of Digital Learning

Contents

ONLINE SAFETY POLICY

1. Introduction

Gayhurst School believes that Computing and IT in the 21st Century has the power to make a significant contribution to teaching and learning across all subjects and ages. We believe the school should be at the forefront of new technologies and promote greater awareness and understanding of the role and uses of technology in the modern world.

We are very aware of the potential problems and issues associated with accessing material available on the internet but see the correct use of internet resources as an essential educational tool in a modern technological society.

Other concerns are the protection of data, security of the network infrastructure, care for the physical equipment, hacking, virus protection and online digital content.

The need for guidelines and rules concerning the use of digital resources at Gayhurst is clearly recognised and, before being allowed to use digital resources, all users must be prepared to accept and abide by the AUP (Acceptable Use Policy) rules laid down by the school, see appendix 5.

Gayhurst believes that the benefits to pupils from access to the resources of the Internet far outweigh the disadvantages. Ultimately, the responsibility for setting and conveying the standards that children are expected to follow when using media and information resources, is one the school shares with parents and guardians.

At Gayhurst, it is felt that the best recipe for success lies in a combination of site filtering, supervision, and the fostering of a responsible attitude in the pupils, in partnership with parents.

All children are required to accept an Acceptable Use Policy (AUP) annually prior to login on a school PC located on the Windows network (Please see appendices). Parents/guardians are made aware of the AUP via this policy, which clearly lays out the expectations the school has of pupils using the Internet at Gayhurst.

Gayhurst School will meet its safeguarding duties under Keeping Children Safe in Education (KCSIE) 2025 by combining: (a) an age-appropriate curriculum for digital resilience; (b) appropriate filtering and monitoring that meets DfE standards; (c) staff training and supervision; and (d) clear reporting and response processes with robust record-keeping. Senior leaders and governors will review the effectiveness of these measures at least termly and after any serious incident.

2. Responsibilities

2.1. Online Safety Lead – Director of Digital Learning

The Online Safety lead will:

- Establish and Lead the Online Safety group
- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL)
- take day-to-day 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 / awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned
- 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 incidents and create a log of incidents to inform future online safety developments
- provide (or identify sources of) training and advice for staff, governors, parents and learners.
- liaise with technical staff, pastoral staff and support staff (as relevant)
- meet regularly with the Safeguarding governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs
- attend relevant governing body meetings/groups
- report regularly to headteacher/senior leadership team.
- Co-author a Filtering & Monitoring Annual Report to governors; include incident trends and improvements.

2.2. Designated Safeguarding Lead (DSL)

The DfE guidance “Keeping Children Safe in Education” states:

“The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety). This should be explicit in the role holder’s job description.” … Training should provide designated safeguarding leads with a good understanding of their own role, … so they … are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college.”

The DSL will therefore:

- Maintain an operational understanding of the school’s filtering and monitoring systems, including how alerts are triaged, false positives handled, and how changes are authorised.

- Termly review filtering/monitoring efficacy with the Online Safety Lead and MSP, report summaries to the safeguarding governor, and record actions.
- Ensure staff CPD reflects current online risks
- Co-author a Filtering & Monitoring Annual Report to governors; include incident trends and improvements.
- Hold an administrative account (or formal change pathway) with the MSP to approve material rule changes; log changes

The DSL will 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

2.3. Heads of Department (HoDs)

The HoDs lead will:

- work with the Online Safety Lead to develop a planned and coordinated online safety education programme

- This will be provided through:
  - PSCHE
  - Discrete computing topics
  - Any opportunities for cross curricular links
  - Assemblies and Pastoral Programmes
  - Relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

2.4. Staff 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 (AUP)
- they immediately report any suspected misuse or problem to the DSL or Online Safety Lead for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers should be on a professional level and only carried out using official school systems
- 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 regarding these devices
- in lessons where internet use is pre-planned 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
- 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.

2.5. External Service Providers (Network Managers – Concero)

Concero are responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy 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
- there is clear, safe, and managed control of user access to networks and devices
- 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 technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to (insert relevant person) 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 monitoring
- software/systems are implemented and regularly updated as agreed in school policies

2.6. Acceptable Use (See Appendix 1)

The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated/re-enforced through:

- Staff induction
- Annual signatures from pupils and their parents

2.7. Reporting and Responding

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 report online safety issues/incidents.
- Reports will be dealt with as soon as is practically possible once they are received.
- The Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- If there is any suspicion that the incident involves any illegal activity or the potential for serious harm, the incident must be escalated through the agreed school safeguarding procedures.
- any concern about staff misuse will be reported to the Head, unless the concern involves the Head, in which case the complaint is referred to the Chair of Governors.
- All concerns are recorded in the school's safeguarding system with date/time, actions, rationale and outcome. Where online content is involved, capture minimal evidential screenshots only where lawful and necessary; avoid re-dissemination.

- If illegal content (CSAM/terrorist material) is suspected, do not download or share; preserve device state and escalate to police/CEOP immediately.

  Where 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.
  - ICT Management company to aid the members of SLT in, and throughout, their investigation to ensure all actions are kept safe, and conducted without exposing the school to unnecessary risk. If the concern is directly related to the ICT Management company then a Senior Member of the company's staff will be involved in the investigation.
  - Conduct the procedure using a designated device 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 device for the duration of the procedure.
  - Ensure that the relevant staff 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.

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:

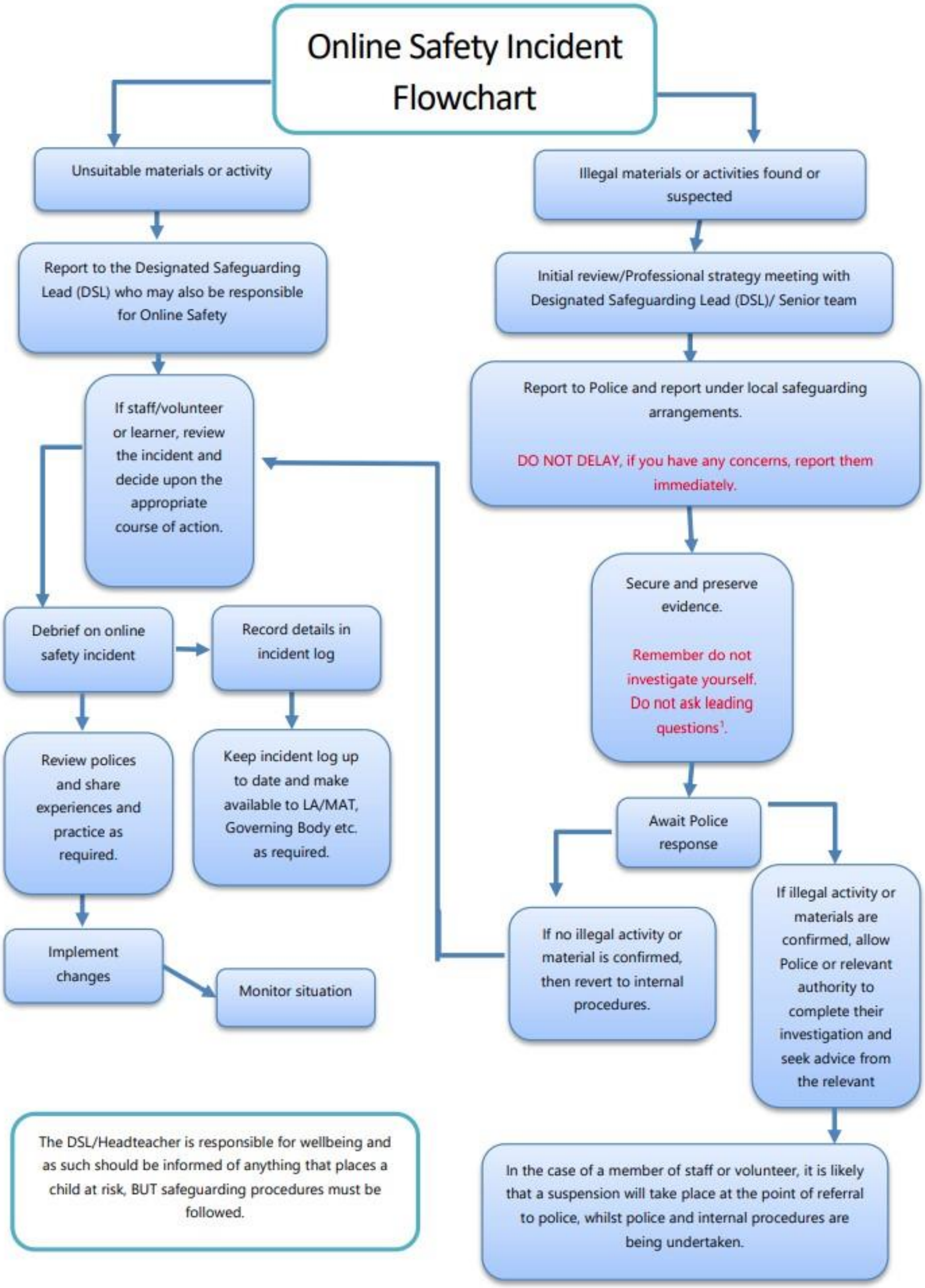
- Internal response or discipline procedures
- police involvement and/or action

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 reporting or affected by an online safety incident. 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 and CEOP.

Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant).

3. Online Safety Incident Flowchart



Online Safety Incident Flowchart

Unsuitable materials or activity

Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety

If staff/volunteer or learner, review the incident and decide upon the appropriate course of action.

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.

Implement changes

Monitor situation

Illegal materials or activities found or suspected

Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team

Report to Police and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not ask leading questions[1].

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

4. Online Safety Training

4.1. Students

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 for all year groups
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital
  pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
- 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 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
- 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
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes – it is mapped to the UKCIS Education of a Connected World.

4.2. Staff

All staff will 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 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.
- 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.

- The Online Safety Lead and Designated Safeguarding Lead (or other nominated person) will receive regular updates through attendance at external training events, 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 guidance/training to individuals as required.

4.3. 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.

A higher level of training will be made available to the Safeguarding Governor.

4.4. Families

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,
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant web sites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers

5. Scams and Phishing Emails

Scams and Phishing Emails Awareness:

In our commitment to fostering a safe online environment for students, staff, and parents, Gayhurst School acknowledges the increasing prevalence of scams and phishing emails. These deceptive practices aim to exploit individuals by tricking them into divulging sensitive information, such as usernames, passwords, or personal details. It is imperative that the community remains vigilant and informed to protect against these potential threats.

Guidelines for Recognizing Scams and Phishing Emails:

Verify Sender Information:

Encourage users to carefully examine the sender's email address. Legitimate communications from Gayhurst School will always come from official domains (e.g. @**gayhurstschool.co.uk or**

@gayhurstschool.onmicrosoft.com).

Be Sceptical of Unsolicited Emails:

Advise users to exercise caution when receiving unexpected emails, especially those requesting personal information, login credentials, or financial details.

Check for Spelling and Grammar:

Remind users that phishing emails often contain spelling and grammatical errors. Genuine communications from **Gayhurst** will maintain a professional and polished language.

Avoid Clicking on Suspicious Links:

Emphasize the importance of refraining from clicking on links or downloading attachments from unknown or unexpected sources. Encourage users to hover over links to preview the actual URL before clicking.

Examine Email Content:

Instruct users to scrutinize the content of emails for inconsistencies. Phishing emails may create a sense of urgency or panic to prompt immediate action.

Reporting Suspected Phishing Attempts:

Inform IT Support:

Encourage users to report any suspicious emails immediately to Concero team at help@concero.education

Avoid Forwarding Suspected Emails:

Remind users not to forward suspicious emails to other recipients before verifying their legitimacy with the IT support team.

Educational Programs:

Regularly conduct awareness sessions and training programs to educate the Gayhurst School community on recognizing and avoiding scams and phishing attempts.

6. Use of Technology

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

6.1. Filtering and Monitoring

Gayhurst takes every practical measure to ensure that pupils do not encounter upsetting, offensive or otherwise inappropriate material on the Internet. Owing to the international scale and linked nature of information available via the Internet, however, it is impossible to guarantee that particular types of material will not appear on a computer screen. Gayhurst cannot accept liability for material accessed, or for any consequences of Internet access.

The following measures have been adopted to help minimise the potential for the pupils to be exposed to unsuitable material (although Gayhurst recognises that no system, based on technology, can be 100% secure):

- 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/behaviours.
- the school manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre Appropriate filtering.
- 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
- younger learners will use child friendly/age-appropriate search engines e.g. SWGfL Swiggle.
- filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. There is a staff lead responsible for managing the monitoring strategy and processes.
- There are effective protocols in place to report abuse/misuse. 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.
- Technical monitoring systems are up to date and managed.
-
- Monitoring covers email, web, search terms, keystroke/visual cues where configured, on school-owned devices on-site and, where feasible, off-site via cloud policies.
- Proactive alerts are reviewed daily on school days; high-severity alerts are triaged within the school day; out-of-hours alerts are handled at the next opening unless immediate risk is indicated.
- Pupil searches default to safe search/YouTube Restricted Mode; exceptions require documented educational need and temporary allow-listing.
- We publish a parent-friendly Filtering & Monitoring Summary on the website.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies strategy informed by the school's risk assessment. These may include:

- Physical monitoring (adult supervision in the classroom) or via Senso or Apple Classroom.
- Internet use is logged and regularly monitored and reviewed.
- Filtering logs are regularly analysed and breaches are reported to senior leaders
- 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.
- Use of a third-party assisted monitoring service to review monitoring logs and report issues to DSL and Online Safety Lead.
- The school maintains a written **Online Safety Risk Assessment** mapping age/stage risks to technical and educational controls; reviewed at least termly.
- We hold a Filtering & Monitoring Statement of Compliance describing: product(s) used, configuration, who can change settings, how incidents are escalated, data retention, and how pupils/staff are informed that monitoring occurs.
- Governors receive an **annual assurance report** with metrics (e.g., alert volumes, categories, response times, trend analysis).

6.2. Device Use

Gayhurst staff are issued with either a Microsoft Surface or Apple iPad device. Other devices such as Personal laptops and iPads should not be used at any time to complete work related tasks. Mobile Phone use is governed by the school's Mobile Device and Camera Policy.

6.3. Digital Photos and Videos

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

- The school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- When using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- Staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices.
- Learners' full names will not be used anywhere on a website or blog, particularly in
- Association with photographs

6.4. Online Publishing

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

- Public-facing website
- Social media
- Online newsletters

The school ensures that online safety policy has been followed 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 least 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.

My School Portal includes an online reporting process for parents and the wider community to register issues and concerns.

7. Data Protection

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

For more information, please review the school's Data Protection Policy.