THE GRAMMAR SCHOOL AT LEEDS
Be Inspired

Online Safety Policy

(including EYFS)

Rationale for the Policy:	There are many benefits for schools around the use of technology, especially as a learning tool. In order to take best advantage of this, we need to provide appropriate guidance to members of the school community on the best use of material and communication online, whilst educating people about its dangers, too.
Policy aim:	To support and guide members of the school community in the safe use of technology.

Author:	DSL
Agreed and Authorised by:	GSAL SLT
Date agreed:	September 2023
To be reviewed:	August 2024

Date of last review:	July 2022
Dates of interim amendments/updates:	

Category:	External
Circulation and publication:	School website

The School runs on FREDIE principles:
Fairness, Respect, Equity, Diversity, Inclusion and Engagement

Contents

1. Scope of the Policy

This Online Safety Policy outlines the commitment of The Grammar School at Leeds to safeguard members of our school community, including Early Years, online in accordance with statutory guidance and best practice.

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 technology systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

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

The breadth of issues classified within online safety is considerable, and concerns can occur both online and offline simultaneously, but can be categorised into four areas of risk:

- content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, misandrist, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g., consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.
- commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams. As a school, we will report concerns to the Anti-Phishing Working Group (https://apwg.org/).

The school will deal with such incidents according to 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.

2. Policy Development, Monitoring and Review

This Online Safety policy is reviewed on an annual basis by a group made up of:

- Members of the Executive Leadership Team
- Online Safety Coordinator (Designated Safeguarding Lead)
- Primary Deputy Head – Pastoral
- Heads of PSHE and Computing
- Network Manager
- Director of External Relations

- Data Protection Lead
- Assistant Head – Digital Learning and Professional Development
- Assistant Head Primary – Digital Learning and Assessment

3. Schedule for Monitoring and Review

The implementation of this Online Safety policy will be monitored by	The Online Safety Group
Monitoring will take place at regular intervals	Once per term
The Safeguarding committee and in turn the Governor's Education along with SLT 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 per year
The Online Safety Policy will be reviewed annually, or more frequently in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be	August 2024
Should serious online safety incidents take place, following consultation with the Designated Safeguarding Lead (DSL) or Vice Principals, the following external persons/agencies should be informed	Duty and Advice Safeguarding Team, LADO, Police, CEOP

4. 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)/filtering
- Internal monitoring data for network activity
- Surveys of:
  - pupils
  - parents and carers
  - staff

5. Policy and Leadership Responsibilities

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 individuals and groups within the school.

5.1 Principal and Senior Leaders

i. The Principal 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 Designated Safeguarding Lead.
ii. The Principal and the Designated Safeguarding Lead should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant school disciplinary procedures)
iii. The Principal is responsible for ensuring that the DSL, who is the online safety officer, and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
iv. The Principal 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. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
v. The GSAL Senior Leadership Team will receive regular monitoring reports from the DSL (Online Safety Officer).
vi. The Principal/senior leaders will work with the safeguarding Governor, DSL and IT service providers in all aspects of filtering and monitoring.

5.2 Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors' Education Committee, receiving regular information about online safety incidents and monitoring reports. A member of the governing body has taken on the role of Safeguarding Governor. The duties of this governor will include:

i. regular meetings with the DSL (Online Safety Co-ordinator).
ii. regular receiving (collated and anonymised) reports of online safety incidents.
iii. checking that provision outlined in the Online Safety Policy (e.g., online safety education provision and staff training is taking place as intended).
iv. ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually (the review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the safeguarding governor) – in-line with the DfE Filtering and Monitoring Standards.
v. reporting to relevant Governors Committee meeting.
vi. receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards.
vii. membership of the school Online Safety Group.

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

5.3 Designated Safeguarding Lead (DSL, including Online Safety Officer)

The DSL will:

i. hold the lead responsibility for online safety, within their safeguarding role.

ii. receive relevant and regularly updated training in online safety to enable them to understand the 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.
iii. meet regularly with the safeguarding governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out.
iv. attend relevant governing body meetings/groups.
v. report regularly to Principal/Senior Leadership Team.
vi. be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
vii. liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety).
viii. lead the Online Safety Group.
ix. receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments and have a leading role in establishing and reviewing the school online safety policies / documents.
x. have a leading role in establishing and reviewing the school online safety policies/documents.
xi. coordinate an overarching awareness of and commitment to online safety education/ awareness raising across the school and beyond.
xii. liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated.
xiii. 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.
xiv. receive reports of online safety incidents and creates a log of incidents to inform future online safety developments.
xv. provide training and advice for staff.
xvi. liaise with the local authority.
xvii. liaise with school technical staff, pastoral staff and support staff (as relevant).
xviii. meet regularly with the Safeguarding Governor to discuss current issues, review incident logs and filtering/change control logs.
xix. receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
    - content
    - contact
    - conduct
    - commerce

5.4 Designated Safeguarding Staff

Designated safeguarding staff will work with curriculum leads in both primary and secondary to develop a planned and coordinated online safety education programme.

This will be provided through:

- a mapped cross-curricular programme
- the PSHE and RSE programmes
- assemblies and pastoral programmes
- relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

5.5 Teaching and Support Staff

Are responsible for ensuring that:

i. they have an up-to-date awareness of online safety matters and of the current school Online Safety Policy and practices.
ii. they understand that online safety is a core part of safeguarding.
iii. they have read, understood, and agreed to the Staff Acceptable Use Policy (AUP).
iv. they immediately report any suspected misuse or problem to the Online Safety Officer for investigation and appropriate action in line with school safeguarding procedures.
v. all digital communications with pupils, parents/carers should be on a professional level and only carried out using official school systems.
vi. online safety issues are embedded in all aspects of the curriculum and other activities.
vii. pupils understand and follow the Online Safety Policy and acceptable use policies.
viii. pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
ix. 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.
x. in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use, and that processes are in place for dealing with any unsuitable material that is found in internet searches.
xi. where lessons take place using live-streaming or video conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in Appendix 6.
xii. they have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.
xiii. 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.

5.6 Network Manager/Technical staff

The Network Manager is responsible for ensuring:

i. that they are aware of and follow the school Online Safety Policy, including the section on Technical Security to carry out their work effectively in line with school policy.
ii. that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
iii. that the school meets required online safety technical requirements.
iv. that users may only access the networks and devices through a properly enforced password protection policy (see Appendix 5).
v. filtering is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
vi. there is clear, safe, and managed control of user access to networks and devices.
vii. that 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.
viii. that the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the Online Safety Officer for investigation and appropriate action.
ix. that monitoring software/systems are implemented and updated as agreed in school policies.

5.7 Pupils

i. Are responsible for using the school digital technology systems in accordance with the age-appropriate pupil acceptable use policy.
ii. Will have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
iii. Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
iv. Should know what to do if they or someone they know feels vulnerable when using online technology.
v. Will be expected to know and understand policies on the use of mobile devices and digital cameras (Appendices 2, 3 and 4). They should also know and understand policies on the taking and using of images and on online bullying.
vi. 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.

5.8 Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners' acceptable use agreement (the school will need to decide if they wish parents/carers to acknowledge these by signature)
- publish information about appropriate use of social media relating to posts concerning the school
- seeking their permissions concerning digital images, cloud services etc.
- parents'/carers' presentation evenings, weekly bulletins, letters, GSAL World and the parent portal

Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of GSAL World, on-line pupil records, and the parent portal
- their children's personal devices in the school
- social media

6. 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 the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to SLT and the Governing Body.

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

i. the production/review/monitoring of the school Online Safety Policy/documents.

ii. the production/review/monitoring of the school filtering policy and requests for filtering changes.
iii. mapping and reviewing the online safety provision – ensuring relevance, breadth and progression.
iv. monitoring network/internet/incident logs.
v. encouraging the contribution of learners to staff awareness, emerging trends and the school online safety provision.
vi. consulting stakeholders – including parents/carers and the pupils about the online safety provision.
vii. monitoring improvement actions identified through use of SWGFL 360 self-review tool.

7. Professional Standards

There is an expectation that required professional standards as laid out in the Staff Code of Conduct and the Staff Acceptable Use Policy will be applied to online safety.

8. Policies

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 should use digital technologies responsibly, protecting themselves and the school and how they should 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 Policies (AUP)

An Acceptable Use Policy is a document that outlines a school's expectations on the responsible use of technology by its users. In most schools they are signed or acknowledged by their staff as part of their conditions of employment. Some may also require learners and parents/carers to sign them, though it is more important for these to be understood and followed rather than just signed. There is a range of acceptable use policies in the appendices.

There are different AUPs which are age and stage appropriate and designed for the relevant stakeholders:

- AUP EYFS pupils (Appendix 2)
- AUP Primary pupils (Appendix 3)
- AUP Senior pupils (Appendix 4)
- AUP Staff (Appendix 1)

Stakeholders are required to understand any updates and familiarise themselves with the content annually, prior to accepting their terms of use.

9. 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:

i. 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. Additionally, there are anonymous reporting systems, both physical and online to report any concerns.
ii. all members of the school community will be made aware of the need to report online safety issues/incidents.
iii. reports will be dealt with as soon as is practically possible once they are received.
iv. the Designated Safeguarding Lead/Online Safety Lead and other members of the safeguarding team have appropriate skills and training to deal with online safety risks.
v. 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 (see Flowchart on page 12).
vi. any concern about staff misuse will be reported to the Principal/Vice Principals unless the concern involves the Principal, in which case the complaint is referred to the Chair of Governors and the Local Authority.
vii. 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.
    - 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
        - involvement by local authority (as relevant)
        - police involvement and/or action

viii. it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively.

ix. there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident.

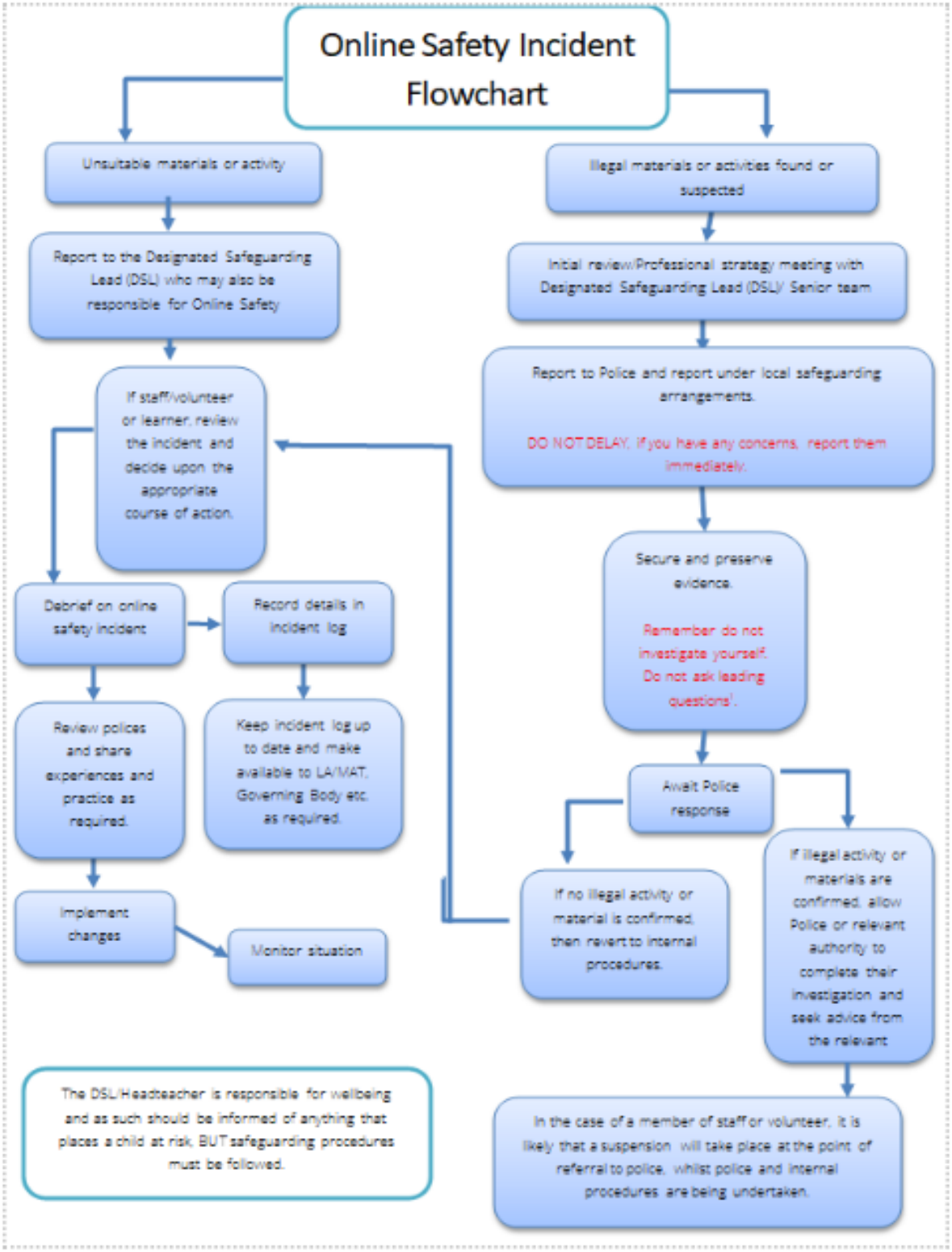
x. incidents are logged on CPOMS.

xi. relevant staff are aware of external sources of support and guidance in dealing with online safety issues.

xii. those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions as appropriate.

xiii. learning from the incident (or pattern of incidents) will be provided as relevant and anonymously 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


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
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.
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!.
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.

10. Online Safety Education

10.1 Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety and digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build 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:

i. A planned online safety curriculum should be provided as part of Computing & PSHE and should be regularly reviewed.
ii. Lessons are matched to need; are age-related and build on prior learning.
iii. Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes.
iv. Pupil need and progress are addressed through effective planning and assessment.
v. Digital competency is planned and effectively threaded through other curriculum areas e.g., PSHE; RSE; Literacy etc.
vi. It incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.
vii. The programme will be accessible to learners at different ages and abilities such as those with individual needs or those with English as an additional language.
viii. Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities (including circle time).
ix. Pupils 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.
x. Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
xi. Pupils 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.
xii. Pupils should be helped to understand the need for the pupil Acceptable Use Policy and encouraged to adopt safe and responsible use both within and outside school.
xiii. Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
xiv. In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
xv. Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
xvi. It is accepted that from time to time, for good educational reasons, pupils 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 Computer Services 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.
xvii. The online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

10.2 Staff

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 training will be made available to 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 should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Policy.
- The Online Safety Officer (DSL) 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 meetings/INSET days.
- Members of the Online Safety Group will provide advice, guidance, and training to individuals as required.

10.3 Governors

Governors should take part in online safety training sessions, with particular importance for those who are members of any subcommittee involved in online safety, health and safety, or safeguarding. This may be offered in a number of ways:

- Attendance at training provided by appropriate, relevant organisations.
- Participation in school training/information sessions for staff or parents.

A higher level of training will be made available to (at least) the safeguarding governor. This will include:

- Cyber-security training (at least at a basic level).
- Training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and review.

10.4 Parents/Carers

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 and regulation of their 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 therefore 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, including reference to websites and publications that may be relevant.
- regular opportunities for engagement with parents/carers on online safety issues through awareness workshops/parent/carer evenings etc.
- Letters, newsletters, websites, parent portal.

- Parent Presentation evenings.
- High profile events and campaigns, e.g., Safer Internet Day.

11. Technology

The school will be responsible for ensuring that the school infrastructure, including the 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.

12. Filtering and Monitoring

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility.

The filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.

Checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and the safeguarding governor, in particular when a safeguarding risk is identified or there is a change in working practice.

12.1 Filtering

i. The school manages access to content across its systems for all users and on all devices using the school's internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre.
ii. 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.
iii. There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective.
iv. There is a clear process in place to deal with requests for filtering changes where staff email flexible@rm.com with requests, ideally in advance of a lesson.
v. The school has (if possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.).
vi. Filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.
vii. Where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.

viii. Access to content through non-browser services (e.g., apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.
ix. If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

12.2 Monitoring

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

i. The school monitors all network use across all its devices and services.
ii. An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored via Smoothwall. Monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead. There is a staff lead responsible for managing the monitoring strategy and processes.
iii. 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.
iv. Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
v. Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

13. Use of digital and video images (inc. Social Media)

This section should be read in conjunction with the separate, 'Taking, Storing and Using images of children Policy.'

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:

i. The school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance/policies – see Appendix 6.
ii. When using digital images, staff will inform and educate students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images.
iii. Staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes. In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their own 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.

iv. Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
v. Care should be taken when sharing digital/video images that learners are appropriately dressed.
vi. Pupils/students must not take, use, share, publish or distribute images of others without their explicit permission.
vii. Photographs published on the school website, or elsewhere that include learners will be selected carefully and will comply with the Online Safety Policy and good practice guidance on the use of such images.
viii. Learners' full names will not be used anywhere on a website or blog, including social media, particularly in association with photographs.
ix. 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. Permission is not required for images taken solely for internal purposes.
x. 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.
xi. Images will be securely stored in line with the school retention policy.
xii. Pupil/student work can only be published with the permission of the pupil/student and parents/carers.

14. Cyberbullying

Cyberbullying is not acceptable. The school adopts a zero tolerance approach to any cyber bullying issues that arise, all staff will challenge any abusive behaviour between pupils that comes to their attention and will report on to the DSL immediately any issues of this nature. All incidents which arise in school will be appropriately investigated and dealt with. Cyberbullying can occur between any members of the school community, and it is important that it is recognised that this is not just a phenomenon which affects pupils. Please see the School's Safeguarding and Child Protection policy for further details about dealing with child-on-child abuse.

The school will educate all members of the community about cyberbullying and should an incident occur, the school will always work to support the victim of cyberbullying. If the incident involves pupils, then reference should also be made to the GSAL Anti-bullying Policy, and the school's Behaviour Policy and the Serious Disciplinary Policy as appropriate.

For incidents involving staff we would follow the Staff Code of Conduct.

- *Cyberbullying: Advice for headteachers and school staff (2014)* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
- *Advice for parents and carers on cyber-bullying (2014)* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/444865/Advice_for_parents_on_cyberbullying.pdf

15. Technical Security

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements:

i. Responsibility for technical security resides with SLT who may delegate activities to identified roles.
ii. There will be regular reviews and audits of the safety and security of school technical systems.
iii. Servers, wireless systems and cabling must be securely located and physical access restricted.
iv. All users will have clearly defined access rights to school technical systems and devices.
v. Details of the access rights available to groups of users will be recorded by the IT service provider and will be reviewed, at least annually, by the SLT/Online Safety Group.
vi. All users (at KS2 and above) will be provided with a username and secure password by Computer Services, who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password. Passwords must comply with the school's password policy (Appendix 5).
vii. The "master/administrator" passwords for the school IT systems, used by the Network Manager (or other person), must also be available to the Principal or other nominated senior leader and kept in a secure place.
viii. Computer Services 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.

16. Mobile Technologies

From October half term 2023, children in Primary school are not allowed to bring a mobile phone to school. Exceptions to this rule is if children have walking permission and if they are travelling on the school bus however, these phones must not be internet enabled devices.

Pupils in Senior School are allowed to bring a mobile phone to school but is not required and it is at their own risk.

The school accepts no responsibility for mobile phones that are lost, damaged or stolen on school premises or transport, during school visits or trips, or while pupils are travelling to and from school.

Mobile phones are not allowed to be used by pupils at any point during the school day unless they have the explicit permission from a member of staff. The exception to this is that sixth form may use their mobile phones but only in the sixth form centre. They must not use it in any other part of the school.

Parents must use the year group administrator as the first point of contact if they need to get in touch with their child during the school day. They must not try to contact their child on their personal mobile during the school day.

Mobile phones should be switched off and carried in the blazer pocket at all times through the school day.

Should a pupil have their mobile phone out or be using it, they will be approached by a member of staff to understand, in the first instance, why they are using it. If no explicit permission has been granted for the person found using their mobile phone, then the phone will be immediately confiscated and taken to Student Support Services where the pupil can the collect it at the end of the school day.

If the phone is confiscated three times, then we will be writing home to parents to look at further sanctions/measures being put in place.

17. Social Media

All adults working with children and young people must understand that the nature and responsibilities of their workplace them in a position of trust and that their conduct should reflect this.

All schools have a duty of care to provide a safe learning environment for learners and staff. Schools 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 liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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.
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
- clear reporting guidance, including responsibilities, procedures, and sanctions.
- risk assessment, including legal risk.
- guidance for learners, parents/carers.

School staff should 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.
- 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, these should be:

- approved by senior leaders.
- clear processes for the administration, moderation, 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 personal social media sites during school hours.

Monitoring of public social media:

As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school.

- The school should effectively respond to social media comments made by others according to a defined policy or process.
- 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 DSL (Online Safety Officer) 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.

18. Online Publishing

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

- Public-facing website
- Social media
- Online newsletters
- My GSAL – school portal

The school website is managed/hosted by the External Relations department. 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.

The school public online publishing provides information about online safety e.g., publishing the schools Online Safety Policy and acceptable use agreements; 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.

19. Data Protection

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

The school:

i. has a Data Protection Policy.
ii. implements the data protection principles and can demonstrate that it does so.
iii. has paid the appropriate fee to the Information Commissioner's Office (ICO).
iv. has appointed an appropriate Data Protection Officer (DPO), who has effective understanding of data protection law and is free from any conflict of interest. The school may also wish to appoint a Data Manager and Systems Controllers to support the DPO.
v. 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.
vi. 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.
vii. has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it.
viii. information asset register 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.
ix. 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.
x. 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.
xi. 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.
xii. has procedures in place to deal with the individual rights of the data subject, e.g., one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them.
xiii. carries out Data Protection Impact Assessments (DPIA) 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.
xiv. has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors.
xv. understands how to share data lawfully and safely with other relevant data controllers.
xvi. has clear and understood policies and routines for the deletion and disposal of data.
xvii. reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
xviii. has a Freedom of Information Policy which sets out how it will deal with FOI requests.
xix. provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular 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:

i. data should be encrypted, and password protected.
ii. device should be password protected
iii. device should be protected by up-to-date endpoint (anti-virus) software.
iv. data will be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Staff must ensure that they:

i. at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
ii. can recognise a possible breach, understand the need for urgency and know who to report it to within the school.
iii. 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.
iv. only use encrypted data storage for personal data.
v. will not transfer any school personal data to personal devices. Procedures should be in place to enable staff to work from home (i.e., VPN access to the school network, or a work laptop provided).
vi. 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.
vii. transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

20. 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:

i. 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.
ii. there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and governors.
iii. parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising.
iv. online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate.
v. 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.

21. School Actions and Sanctions

For incidents involving pupils, we would follow the school's Behaviour Policy and the Serious Disciplinary Policy as appropriate. For incidents involving staff, we would follow the Staff Code of Conduct.

22. Acknowledgements

This policy is based upon the South West Grid for Learning 2023.

Appendices

Appendix 1: AUP Staff

Introduction

The school recognises that digital technology and the internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practise good online safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

Staff at GSAL are expected to be professional and exhibit good behaviour in their use of the school network at all times. Ultimately GSAL owns the computer network and sets both the guidelines for its use and sanctions for misuse. Staff are expected to respect the equipment provided by school and to abide by the various policies concerning the use of computers at GSAL. This applies to all staff working in the school whether paid or unpaid, whatever their position, role or responsibilities and includes employees, governors, supply staff, casual workers, contractors, work experience students and volunteers.

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

Staff should expect that violation of the rules below will result in a ban on computer and network use and may include other disciplinary action in accordance with the School's Discipline Procedure Policy. When applicable, the Police or local authorities may be involved.

Principles

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

The same principles apply when using all platforms and means of access to online activity whilst at work.

At GSAL, we are:

- Responsible for our behaviour (Conduct)
- Aware how we interact with others (Contact)
- Safe with the materials we use and create (Content)
- Aware that risks from things like online gambling, inappropriate advertising, phishing or financial scams can happen (Commerce)

This policy should be read in conjunction with the following GSAL School policies:

- Child Protection and Safeguarding Children Policy
- Serious Discipline Policy and Procedures
- Searching Electronic Devices Policy
- Staff Code of Conduct

- Taking, Storing and Using Images of children policy
- Data Protection Policy
- Password Policy (Appendix 5)
- Email Policy

Personal Safety

1. Staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for education, personal and recreational use.
2. GSAL ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
3. This policy is intended to ensure that staff are protected from potential risk in their use of ICT in their everyday world
4. Staff know and understand that the school will monitor use of the systems, devices and digital communications. The Executive Team and Head of HR are alerted to any alerts of concern about a user's safety or the safety of children using an external company called Smoothwall.
5. Staff will keep their username and password safe and secure for any online account – staff will not share it, nor will they try to use any other person's username and password. Staff understand that they should not write down or store a password where it is possible that someone may steal it. Staff should ensure that their password conforms with the Password Policy at GSAL.
6. Staff should not give their personal contact details to students, including email addresses, home or mobile telephone numbers, unless the need to do so is agreed with the Designated Safeguarding Lead and parents, guardians or carers. Details of this are as outlined in the Staff Code of Conduct.
7. Do not leave any computer unattended with an open (logged on) session. This also applies to remote sessions on portable devices or from home. If staff need to leave a computer briefly, they should lock the session. For longer periods unattended, staff should log off from the computer.
8. Staff will immediately report any illegal, inappropriate or harmful material or incident they become aware of to the Designated Safeguarding Lead (DSL) or a nominated safeguarding officer.

Interacting with others

1. Staff will not attempt to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
2. Staff will not engage in any online activity that may compromise their professional responsibilities.
3. Staff will not access, copy or otherwise alter any other user's files, without their express permission.
4. Staff will be polite and professional when communicating with others; they will not use strong, aggressive or inappropriate language and will appreciate that others may have different opinions.
5. Staff will ensure that when they take and/or publish images of others, they will do so with permission and in accordance with the school's policy of the use of digital/video images. Where images are published (e.g. on the school website/GSAL World) it will not be possible to identify by full name, or other personal information, those pupils who are featured.
6. Staff know that it is a criminal offence to possess, manufacture or distribute indecent images and videos of children (under the age of 18).

7. Staff will only use chat and social networking sites in school in accordance with the school's policies and the Staff Code of Conduct.
8. Staff will only communicate in a professional capacity with students and parents using official school systems. Any such communication will be professional in tone and manner. Staff should be made aware of the risks attached to using their personal email addresses/mobile phones/social networking sites for such communications.
9. GSAL staff are encouraged to activate their own 'Out of Office' message when away from school for more than one working day. This message can also be activated remotely from Outlook Web Access if a member of staff is ill.

Maintaining the security and integrity of the technology GSAL offers and ensuring the smooth running of the GSAL systems

1. Access to educational computing facilities is managed by the Computer Services Department. Equipment is allocated to individuals and/or departments by GSAL Computer Services and the use of any of GSAL computing facilities is at the discretion of the school.
2. The Computing facilities are owned by GSAL and software and/or data developed or created (for whatever reason) on that equipment remain in all respects the property of GSAL. The Patents Act 1977 and the Copyright, Designs and Patents Act 1988 provide for the Intellectual Property Rights (IPR) in that work created by an employee in the course of his/her employment is vested automatically to the employer.
3. Desktop PCs and school owned laptops are a critical asset to GSAL and must be managed carefully to maintain security, data integrity and efficiency. Users must never install software on or modify the hardware of any GSAL owned device without the written permission of the Computer Services Department.
4. Laptop PCs and tablets are at high risk from loss or theft and require additional security protection, including encryption of hard disk drives where possible. All reasonable precautions must be taken to ensure that such hardware is stored securely. Also, to protect the integrity of GSAL systems and data procedures, passwords or authentication devices for gaining remote access to GSAL systems must not be stored with the computer. This includes the saving of passwords into remote access software. If your Laptop, PC or tablet is lost or stolen, the Computer Services Department must be notified as soon as possible and a report made to the Police and the Director of Finance.
5. Loan equipment is similar to that for laptops and tablets. Most loan equipment is highly portable and attractive to thieves. Users who borrow loan equipment bear the responsibility for its care. Loan equipment should be concealed and stored securely when not in use. If loan equipment is stolen or lost, the Computer Services Department must be notified as soon as possible and a report made to the Police and the Director of Finance.
6. Only software properly approved by the IT Strategy group and the Computer Services Department prior to purchase or download may be used on GSAL hardware. If a member of staff is unsure about whether they can install additional apps, they should in the first instance check with Computer Services prior to installation. Non-standard or unauthorised software can cause problems with the stability of computing hardware. The copying and use of software without the licensor's permission is illegal. GSAL has licences to provide certain software titles to staff for use on their own hardware whilst employed at GSAL. When employment ceases the software must be removed.
7. Whilst it is the user's responsibility to take reasonable care over the configuration of their computer hardware, it is possible for software to be installed on a machine without the full comprehension of the user. Users discovering software that has been installed in an unsolicited manner must contact the Computer Services Department who will assist in resolving any issues.

8. Staff will not disable or cause any damage to school equipment or the equipment belonging to others.
9. Staff understand the risks and will not try to upload, download or access any material which is illegal or inappropriate or may cause harm or distress to others, nor will they use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.
10. Staff will promptly report any damage or faults involving equipment or software, however this may have happened.
11. Staff will not open any hyperlinks in emails or any attachments to emails, unless they know and trust the person/organisation who sent the email, or if staff have concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes). If a staff member suspects that they have a virus, Trojan or ransom ware infection on their PC/laptop, they should shut the device down immediately and remove it from the wired and wireless network before seeking urgent assistance from Computer Services.
12. Staff will ensure that their data are regularly backed up. Note that key data on the school network are protected by regular automatic back-ups.
13. Staff will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. Staff will not try to use any programmes or software that might allow them to bypass the filtering and security systems in place to prevent access to such materials.

Responsible for their behaviour, both in and out of school

1. The use of personal devices, wirelessly connected to the network, is allowed by all members of staff. Do not use wired connections from personal devices to the network (also see 5.11.)
2. Staff understand that GSAL also has the right to take action against them if they are involved in incidents of inappropriate behaviour, that are covered in this agreement, when they are out of school and where they involve their membership to the school community (examples would be online bullying, use of images or personal information).
3. Staff understand that the data protection policy requires that any staff or student data to which they have access will be kept private and confidential, except when it is deemed necessary that they are required by law or by school policy to disclose such information to an appropriate authority.
4. Staff should ensure that their activity online is not defamatory and does not bring the school's name into disrepute, e.g. making defamatory comments about individuals, other organisations or groups, the GSAL; or posting images that are inappropriate, links to inappropriate content or using inappropriate language.
5. Staff understand that if they fail to comply with this Acceptable Use Policy Agreement, they may be subject to disciplinary action. This may include amongst other potential measures the loss of access to the school network/internet, suspensions, and in the event of illegal activities involvement of the Police.

Use of Digital and Video Images

1. Staff understand the primary purpose of having their portable device at school is educational, irrespective of whether the device is school owned or personal.
2. Staff need to be aware of the risks associated with publishing digital images on the internet. Those images may provide an avenue 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.

3. In accordance with guidance from the Information Commissioner's Office, parents/guardians 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 should not be published/made publically available on social networking sites, nor should parents/guardians comment on any activities involving other pupils in the digital/video images.
4. Staff are allowed to use school cameras and devices (but see 5.8. in addition) to record pupils' learning and attainment and any images should be appropriately stored solely on the school network and are not to be removed from the premises unless authorised and having been considered for appropriate use. In the event of images taken on tablet or other portable devices, or away from school, these should be uploaded to the appropriate school system and then deleted from the device at the first opportunity.
5. Staff who work in a one-to-one situation with students should be mindful when taking photographs; this should be relevant and appropriate to the needs of the child.
6. Video, audio and photographic recording must never take place without the consent of student(s) and teacher(s). Consent must be explicit, not implied.
7. Permission must be sought for the capture of images in areas which may be deemed to be sensitive, e.g. swimming pool. Staff should at all times ensure that all images they take or commission to be taken are wholly appropriate. Where an image inadvertently contains something which may be viewed as inappropriate, e.g. an unfortunate camera angle, this should be taken to the DSL immediately in a spirit of transparency so that this may be addressed immediately.
8. The use of personal devices to record or photograph pupils should be avoided if at all possible. If an image is taken using a personal device, the data must be downloaded onto the School network as soon as is possible and then deleted from the device and any other personal storage locations. This should happen before taking the personal device home.
9. Photographs published on the website or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

Use of personally owned devices

1. Staff must not connect any personal device to the wired network.
2. Staff may connect personal devices to the GSAL Staff WiFi network. However, those devices are subject to the same restrictions as any other device connected to the network and their use will be monitored as with school owned devices.
3. Staff personal devices are brought into school entirely at the risk of the owner and the decision to bring the device in to the school lies with the member of staff as does the liability for any loss or damage resulting from the use of the device in school.
4. Users are responsible for keeping their personal devices up to date through software, security and application updates. The device is virus protected and should not be capable of passing on infections to the network. Devices which do compromise the network will be blocked and the associated user account disabled.
5. The school accepts no responsibility or liability in respect of lost, stolen or damaged personal devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home).
6. The school accepts no responsibility for any malfunction of a personal device due to changes made to the device while on the school network or whilst resolving any connectivity issues

7. The school recommends that personal devices are made easily identifiable and have a protective case to help secure them as the devices are moved around school.
8. Passcodes or PINs must be set on personal devices to aid security. It is not recommended that staff use USB sticks to transfer data. If these must be used then they, these should be encrypted.
9. The school is not responsible for the day-to-day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.
10. Social media and messaging should only be used in compliance with the Staff Code of Conduct, and never for sending personal messages to students.

Managing emerging technologies

- Technology is progressing rapidly and new technologies are emerging all the time. The school will risk- assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have.
- The school keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for taking advantage of and dealing with new technological developments.

Staff Acceptable Use Policy

- All staff members are required to agree to the acceptable use policy as an intrinsic and necessary part of their employment at the school.
- All staff members provide this consent electronically on an annual basis as part of their regular log on procedure. By electronically consenting to the Staff AUP, staff members indicate that they have read, understood and agree to the Staff Acceptable Use Policy.

This policy is based on the 2023 template produced by South West Grid for Learning Trust.

Appendix 2: AUP for EYFS Primary Pupils (Nursery/Reception)

Acceptable use policy

I will ask an adult if I want to use the computers/tablets.

I will only use activities that an adult has told or allowed me to use.

I will take care of computers/tablets and other equipment.

I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.

I will tell an adult if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer/tablet.

Appendix 3: AUP Primary Pupils (Y1-6)

Using computers and tablets is a part of everyday life inside and outside school. They can help support your studying in school in exciting ways. All children should be able to use computers, tablets, and the internet safely.

Your Class Teacher will review this form with you, and if you have any questions you should talk to your Class Teacher and parents about them.

This is how we stay safe when we use computers:

The school monitors what I do when I am using a school computer or tablet, and my parent/guardian may be contacted if a member of school staff is concerned about my safety or behaviour.

- I will ask a teacher or suitable adult if I want to use the computers or tablets.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will only send teachers emails from my school email address.
- I will not tell other people my ICT password.
- When I am using a computer or tablet, I will not give out personal details, such as: my name, my phone number; or my home address.
- I will not spoil or delete anyone's work.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible. I will never be unkind or rude.
- I will not look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher immediately.
- I know that some people online may lie about who they are and that some of the information on the web is not true. I will be careful about who and what I believe, and will speak to a teacher if I am worried.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell my teacher or parent if something makes me worried or uncomfortable, or if I believe that someone is being bullied online.
- I will shut the screen and then immediately tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer or tablet.

This policy is based on the 2023 template produced by South West Grid for Learning Trust.

Appendix 4: AUP Senior Pupils

Introduction

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

All Senior School pupils are issued with a laptop by the school. It is the pupils' responsibility to look after this device, bring it to lessons, and ensure it is charged and ready for use when in school. Pupils with ICT queries or difficulties should contact Computer Services.

This Acceptable Use Policy is intended to ensure:

- that GSAL Senior School pupils will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that GSAL systems and users are: protected from accidental or deliberate misuse that could put the security of the systems at risk; and will have good access to digital technologies to enhance their learning and in return, we expect the pupils to agree to be responsible users.

Acceptable Use Policy Agreement

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

For my own personal safety:

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

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

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing.
- I will not use the school systems for video broadcasting (e.g., YouTube), unless I have permission of a member of staff to do so.

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

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

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

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

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

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

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

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this policy, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy, I will be subject to disciplinary action. This may include: loss of access to the school network, and the internet

while in school; detentions; exclusions; contact with parents; and, in the event of illegal activities, pupils should expect that the school would involve the police.

Every year, when the policy has been updated, you will go through this policy with your Form Tutor or Head of Year. Following this, on an agreed date, when you first log on to a computer in school, you will be asked to agree that you have read, understood and agree to abide by the rules included within this Acceptable Use Policy. If you are not happy with any aspect of this Acceptable Use Policy, please speak with your Form Tutor or Head of Year in the first instance and before your first log on to the School System, and any first log on following an update to this Acceptable Use Policy. If you do not agree to abide by this Acceptable Use Policy, access will not be granted to school systems and devices.

This policy is based on the 2023 template produced by South West Grid for Learning Trust.

Appendix 5: Password Policy

Introduction and Password Security

At GSAL we seek to educate young people in the need to keep online or network access secure, and to protect the online or networked environment from data protection and cyber-security breaches.

1. Staff and pupils will keep their username and password safe and secure for any online account – they will not share them, nor will they try to use any other person's username or password. Staff and pupils understand that they should not write down or store a password where it is possible that someone may steal it.
2. Any device (including, but not limited to, personally owned mobile phones and computers) through which school systems are accessed must be appropriately password protected.
3. Following guidance on best practice from the National Cyber Security Centre, staff and pupils are not required to change their password except where the security of their password may have been compromised. However, staff and pupils are required to adhere to the guidelines on 'complexity' as set out in this policy.
4. Staff and pupils should inform Computer Services if they suspect their password has been compromised, so that a new password can be arranged and implemented.
5. Passwords used for school-related systems must not also be used for personal, non school-related, accounts.
6. To stop "brute force" attacks where passwords are repeatedly entered by automated systems an account lockout policy will be implemented. After entering a password incorrectly 10 times consecutively the account will be locked. The account will automatically unlock after 40 minutes. The Computing Services helpdesk will be able to unlock accounts when needed.

GSAL Password Complexity

Early Years Foundation Stage

Within EYFS, computers are only used as an access to educational software and are accessed via a year group username and password suitable for 3-5 year olds to quickly memorise and be able to input using a keyboard.

Key stage 1

Computers continue to be used for access to educational software. At this stage each class has its own login following similar rules to EYFS

Year 2 pupils will be given a personal username and password during the summer term which they will use from year 3. These will be kept on a spreadsheet by year 2 staff to support the children to memorise their details ready for year 3.

Key stage 2

Primary school usernames consist of a 6 digit number, which remains consistent throughout the child's time at GSAL (including their senior school years) all children from this age also receive an email account.

Year 6 pupils choose a new 8 digit password during the summer term in preparation for their move to the senior school (see 'senior school', below).

Senior school

Senior school usernames consist of a 6-digit number, which remains consistent throughout the pupil's time at GSAL. All senior school pupils are required to have an 8-digit password **which includes at least one number and at least one symbol** within the password.

Staff

Staff should create a password of a minimum length of 16 digits. It is recommended practice that staff use 4 random words each of at least 4 letters long, and either substitute some letters for symbols or numbers, or add numbers/symbols to the beginning or end, or in-between words. However, this should not then make the password too difficult to remember, resulting in it being written down.

Multi-factor authentication was put in place for staff Microsoft accounts during the academic year 2020-2021 and will be in place from this point forward.

Note: Please do not use the examples given below

e.g., roaDjadeboatlime – this is the minimum complexity as it has no numbers or special characters

Recommended complexity adds in numbers, words of more than 4 characters and special characters:

e.g., Show-Ball-Fr0g-Ha!l
e.g., banglemonPau!fish
e.g., Bank.Tree.5uit.Ba££

For those struggling, there are a number of websites that can generate random words – for example:
http://correcthorsebatterystaple.net/ or
http://listofrandomwords.com/index.cfm?nlist

Related Policies and Documents

- Data Protection Policy
- Staff Acceptable Use Policy
- Acceptable Use Policy Senior Pupils
- Acceptable Use Policy Primary Pupils

Appendix 6: Video Conferencing

Introduction

Video conferencing and associated chat facilities are used at The Grammar School at Leeds: to teach remotely; and hold meetings. The use of video conferencing can benefit everyone in the school community but it is important that the use of video conferencing is treated in a responsible fashion and that staff, pupils, and parents use it responsibly and practise good online safety.

This policy outlines how staff, pupils, and parents are expected to interact with each other through video conferencing. Violation of this policy will be dealt with in accordance with: the relevant pupil disciplinary policies; staff code of conduct and disciplinary policy.

Principles

All members of the school community should understand that they use video conferencing in a responsible way, to ensure that there is no risk to their safety or to the safety and security of the school's ICT systems and other users.

At GSAL, we are:

- Responsible for our behaviour (Conduct)
- Aware how we interact with others (Contact)
- Safe with the materials we use and create (Content)
- Aware that risks from things like online gambling, inappropriate advertising, phishing or financial scams can happen (Commerce)

This appendix should be read in conjunction with the rest of this policy and its appendices, and the following GSAL School policies:

- Safeguarding Children and Child Protecton Policy
- Staff Code of Conduct
- Disciplinary Policy
- Data Protection Policy

Use of Video Conferencing for all staff (meetings and live teaching sessions)

1. Staff will ensure that all video conferencing meetings and live teaching sessions are set up in line with the guidance provided within this policy;
2. Staff will refer to the appropriate GSAL guidance for the video conferencing platform they are using;
3. Staff will ensure appropriate dress at all times when attending a meeting or live teaching session. At a minimum this should be clothes acceptable on "own clothes" day or the GSAL PE kit;
4. Staff will ensure that they use a backdrop when using video or that they are in an area of their home without personal objects, such as photographs or other personal information, in the background;
5. Staff will must ensure that their environment is appropriate for the meeting or live teaching session which is taking place, and that no sensitive or personal information can be overheard by anyone who is not entitled or appropriate to have that information shared with them. If the environment is not appropriate the meeting should not go ahead without measures to ensure the meeting can take place appropriately being put in place, such as others being asked to leave the area, headphones being worn, or the location changed.;
6. At present, only staff accounts with Microsoft Teams and Zoom are to be used for video conferencing, other platforms should not be used without the express permission from the relevant SLT;

7. Staff will ensure that other members within their household do not have access to their school accounts or have the ability to access any of the meetings or live teaching sessions;
8. Staff are permitted to record meetings attended by staff only for training purposes or to record meetings with pupils for safeguarding purposes. Before recording a meeting the host must obtain the explicit consent of every individual in attendance and document this. If any attendee refuses consent the meeting **must not** be recorded and that individual must not experience any discrimination, for example, be removed from the meeting so that it can be recorded. Any recordings must be stored locally on the user's GSAL issued device or on the GSAL network, on a GSAL Microsoft account (note, recordings should not be stored on Zoom's own servers).
9. Staff must not post links to meetings or the meeting ID publicly. Staff must send the link direct to trusted individuals or groups.

Use of video conferencing for primary teaching

1. Staff must use the waiting room feature for all live teaching sessions. If a teaching session contains a large number of pupils, a second adult should be in attendance. One of the adults must be responsible for admitting attendees once they recognise their name. If they don't recognise the name, they should admit them but check immediately that they recognise the face that has appeared in the video and if they don't, remove that attendee.
2. Staff must not record any live teaching session with pupils.
3. For sessions in which only one teacher is present, staff must follow the following rules:
    - three or more children - continue as normal
    - two children - ask for the parents of each child to be present
    - one child - re-schedule
4. If there are two teachers on the Zoom call, staff can continue with any number of children.
5. If staff experience anything that causes concern during a live teaching session, the session must be stopped immediately and an appropriate member of SLT informed immediately of what has happened
6. Staff must not talk to parents during live teaching sessions
7. Parents should not get involved with the video conferencing sessions but leave the children to interact with the teachers and their classmates
8. Parents should email staff using the year group emails if they wish to speak to a member of staff. Parents should not use the live teaching sessions for this purpose
9. Parents will ensure their child is appropriately dressed for the remote live video session
10. Parents and pupils should be mindful that the microphone and camera could pick up background noises and images from your household. Pupils should be sat in an appropriate location to minimise this
11. Parents and pupils must not record the live teaching sessions
12. Parents and pupils must not share the meeting link, password or meeting ID with any other individual