BUCKINGHAMSHIRE COUNCIL

Online Safety Policy
Tylers Green Middle School

This policy was adopted on: Autumn 2025

The policy is to be reviewed by: Autumn 2026

Contents

1. Development/Monitoring/Review of this Policy

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

- Acceptable Use
- AI Principles
- Anti-bullying
- Behaviour
- Child Protection
- Data Protection
- PSHE
- Staff Code of Conduct
- Visitors
- Volunteers

This Online Safety Policy has been developed by a working group/committee made up of:

- Headteacher
- Online Safety Coordinators
- Staff – including teachers, support staff, technical staff
- Governors
- Parents and carers

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

In line with emerging national evidence on the impact of early smartphone and social media exposure on childhood development, and following DfE, Ofsted, and UK Safer Internet guidance encouraging schools to support parents with digital safeguarding and healthy tech habits, Tylers Green Middle School is working with the Chiltern Area Partnership (CAP) to establish a shared Guiding Digital Childhoods (GDC) approach.

While not a statutory requirement, this work reflects current best practice in online safety leadership and aligns with our duty to promote pupil welfare and resilience (KCSIE, Education Act 2002, Online Safety Guidance 2023). This policy, therefore, includes a GDC Addendum, offering developmental guidance for families and clarifying our collective action commitments as a CAP school (Appendix 6).

Alongside the other 11 CAP schools, Tylers Green Middle School is committed to supporting children's healthy development and digital well-being through promoting the **Four Guiding Principles for Families** and **Four Commitments for Schools**, which are the foundations of our taught curriculum.

Guiding Principles for Families:

- 📵 **Delay smartphones until at least Year 9** to allow children to develop social skills and independence free from constant connectivity.
- 🚫 **Delay social media until at least age 16** to reduce exposure to harmful comparison, anxiety, and algorithmic content during vulnerable developmental stages.
- 🏫 **Phone-free schools** to ensure the school day is focused on learning, play, friendship, and face-to-face communication.
- 🌳 **More independence, free play, and responsibility in the real world** to prioritise outdoor play, unstructured time, and real-world experiences as protective factors for good mental health.

School Commitments:

- We will remain **phone-free for pupils throughout the school day**.
- We will **actively teach digital safety, literacy, mindfulness and responsibility** across the curriculum.
- We will **provide consistent guidance, resources and workshops** to support parents.
- We will **model and promote healthy tech use** as a staff body and school culture.

Schedule for Development/Monitoring/Review

This online safety policy was approved by the Governing Body on:	*20th November 2025*
The implementation of this online safety policy will be monitored by the:	*S Isaacs – Online Safety Lead* *C Johnson & U Bawany – Online Safety Coordinators* *K Dudley - Governor for Online Safety* *E Barlow – Governor for Safeguarding*
Monitoring will take place at regular intervals:	*Annually*
The Governing Body will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Termly*
The online safety policy will be reviewed annually, or more regularly 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:	*Autumn 2024*
Should serious online safety incidents take place, the following external persons should be informed:	*LA Safeguarding Officer, LADO, Police*

The school will monitor the impact of the policy using:

- CPOMS logs of reported incidents

- The school's ICT provider's (EAC) monitoring logs of internet activity (including sites visited)/filtering
- Internal monitoring data for network activity
- Surveys/questionnaires of
    - students/pupils
    - parents/carers
    - staff

2. Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students/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 deletion of data (Acceptable User Agreement). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.
The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place outside of school.

3. Roles and Responsibilities

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

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 receiving regular information about online safety incidents and monitoring reports. The school has a designated Safeguarding Governor and a separate Online Safety Governor. The role of the Online Safety Governor will include:

- Meetings with the Online Safety Lead
- Attendance at Online Safety Group meetings
- Regular monitoring of online safety incident logs
- Regular monitoring of filtering/change control logs
- Reporting to relevant Governor meetings (Teaching and Learning Committee)
- Liaising with the chair of governors to provide e-safety training for all governors

Headteacher and the Online Safety Lead

- The Headteacher is also the Online Safety Lead and has a duty of care for ensuring the safety (including online safety) of members of the school community
- The Headteacher and both assistant headteachers 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 Local Authority disciplinary procedures)
- The Headteacher/OSL is responsible for ensuring that relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant
- The Online Safety Governor and the Headteacher/OSL will ensure those in school who carry out the internal online safety monitoring role (Online Safety Coordinators) are supported through the termly Online Safety Group meetings
- Leads the Online Safety Group
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Liaises with the local authority
- Liaises with school technical staff
- Receives reports of online safety incidents through CPOMS
- Meets with the Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- Attends relevant meetings of governors
- All incidents will be dealt with in accordance with the online safety policy and the behaviour policy

Online Safety Coordinators

The Online Safety Coordinators are named on Pages 2 and 3.

- The Online Safety Coordinators are responsible for determining, evaluating and reviewing online safety policies to encompass teaching and learning, and the use of school ICT equipment and facilities by pupils, staff and visitors. They are also responsible for agreeing on the criteria for acceptable use by pupils, school staff and governors of internet-capable equipment for school-related purposes or in situations which will impact on the reputation of the school, and/or on school premises
- The OSCs will use the School self-evaluation process and Development Plan to set clear objectives and strategies for online safety provision which will deliver measurable success via a calendar of online safety provision
- Takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the school's online safety policies/documents
- Provide training and advice for staff

- Provide adequate provision of online safety education for pupils
- Liaise with external ICT contractors [EAC]
- Liaise with the Online Safety Lead on incidents reported through CPOMS

Network Manager/Technical staff

The school works with EAC as an external ICT contractor. EAC are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required online safety technical requirements and any local authority online safety policy/guidance that may apply.
- That Users may only access the networks and devices through their individual protected password which they agree to in the acceptable user agreement signed annually
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person. At TGMS, this is done by Sophos which is live and constantly updated
- 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
- That the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the ICT lead and the headteacher/Online Safety Lead for investigation/action/sanction - updates from Sophos on filtering (reports what has been blocked)
- That monitoring software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current school online safety policy and practices
- They have read, understood and signed the staff Acceptable Use Agreement
- They report any suspected misuse or problem to the Online Safety Coordinators for investigation/action and eventual sanctions through the Online Safety Lead
- All digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the Acceptable Use Agreement (Appendix 2)
- Pupils have a good understanding of research skills and the need to avoid plagiarism
- They monitor the use of digital technologies, mobile devices, cameras, etc. In lessons and other school activities (where allowed) and implement current policies with regard to these devices

- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead (DSL)

The school has a Designated Safeguarding Lead (Headteacher) who is trained in online safety issues and is aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming
- Online-bullying

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the online safety policy, including the impact of initiatives. The Online Safety Group will include representation from pupils (Digital Leaders), parents /carers, governors, teaching staff, support staff, office, technical support team and SLT. They will need to read and agree to the Online Safety Group's terms of reference. The group will also be responsible for regular reporting to the governing body/directors.

Members of the Online Safety Group (Digital Leaders, when appropriate) will assist the Online Safety Lead with:

- The production/review/monitoring of the school's online safety policy/documents.
- The production/review/monitoring of the school filtering policy (if the school chooses to have one) and requests for filtering changes. This is Sophos as above
- Mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression
- Monitoring network/internet/filtering/incident logs EAC to monitor network, libra for emails, Sophos filtering, a different part of Sophos that produces monitoring alerts that get flagged to EAC as a ticket, Sophos contacts EAC if they think they have seen an attack
- Consulting stakeholders – including parents/carers and the students/pupils about the online safety provision
- Monitoring improvement actions identified through the use of the 360-degree safe self-review tool

Students/pupils:

- Are responsible for using the school digital technology systems in accordance with the student/pupil acceptable use agreement

- Have a good understanding of research skills and the need to avoid plagiarism.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and online bullying
- Should understand the importance of adopting good online safety practices 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 in the school

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 parents' evenings, newsletters, letters, the website, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practices and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website/Learning Platform and online student/pupil records
- Their children's personal devices in the school (where this is allowed)

4. Policy Statements

Education – Students/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/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.

In planning the online safety curriculum, the school will refer to the guidelines set out in the DfE Teaching Online Safety in Schools.

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

A planned online safety curriculum should be provided as part of Computing/PSHE/other lessons and should be regularly revisited.

- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities

- 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
- Pupils may be challenged, if deemed appropriate for their ability, to acknowledge the source of information used
- 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
- Pupils should be helped to understand the need for the pupil-acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons, where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that filters and blocks are in place for dealing with any unsuitable material that is found in internet searches
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated persons) 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
- Given the rise of generative AI and its potential to contribute to misinformation, deep-fakes and privacy concerns, pupils will be made aware of the following:
    - AI-generated content: Ensuring that students understand how AI can be used to create misleading or fake content and are educated on how to critically evaluate sources.
    - Deep-fakes: A specific focus on AI's role in creating highly realistic but false images, videos, or information.
    - Ethical AI use: Teaching students the ethical implications of using AI tools responsibly in generating content themselves.

Education – 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/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities

- Letters, newsletters, website, Learning Platform
- Parents/carers evenings/sessions
- High-profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant websites/publications e.g.
  - www.swgfl.org.uk
  - www.saferinternet.org.uk
  - www.childnet.com/parents-and-carers

Education – The Wider Community

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

- Providing family learning courses in the use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents
- The school website will provide online safety information for the wider community
- Sharing their online safety expertise/good practice with other local schools through participating in the Wycombe North Liaison Group and other ongoing school-to-school partnerships, for example with Tylers Green First School and the Chiltern Area Partnership
- Supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their online safety provision (possibly supporting the group in the use of Online Compass, an online safety self-review tool for groups such as these - www.onlinecompass.org.uk)

Education & Training – Staff/Volunteers

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

- An annual planned programme of formal Online Safety training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly by an Online Safety Coordinator
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school's online safety policy and acceptable use agreements. Online Safety BOOST includes an array of presentations and resources that can be presented to new staff (https://boost.swgfl.org.uk/)
- It is expected that some staff will identify online safety as a training need within the performance management process

- The Online Safety Lead and the Online Safety Coordinators will receive regular updates through attendance at external training events (e.g. from SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations
- This online safety policy and its updates will be presented to and discussed by staff in staff meetings/training sessions
- The Online Safety Lead will provide advice/guidance/training to individuals as required. Online Safety BOOST includes an array of presentation resources that the Online Safety Lead can access to deliver to staff https://boost.swgfl.org.uk/. It includes presenter notes to make it easy to confidently cascade to all staff

Training – Governors

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

- Attendance at training provided by the Local Authority/MAT/National Governors Association/or other relevant organisation (e.g. SWGfL)
- Participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons)

Technical – Infrastructure/equipment, filtering and monitoring

TGMS has a managed ICT service provided by an outside contractor (EAC), and it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school, as suggested below. The managed service provider is fully aware of the school's Online Safety Policy/Acceptable Use Agreements

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It also ensures that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- The school's technical systems will be managed in ways that ensure that the school meets the recommended technical requirements outlined by the Local Authority
- There will be regular reviews and audits of the safety and security of the school's technical systems by the school and external provider (EAC)
- Through EAC, the school use the cloud-based Securly and Sophos software, providing monitoring and filtering tools to help schools ensure online safety for students. It filters inappropriate content, monitors online activity, and flags concerning behaviour, such as cyberbullying or self-harm risks with the school's Designated Safeguarding Leads and ICT and Communications Coordinator. Both services aim to create a safer digital environment by giving schools real-time visibility into students' online interactions while respecting privacy policies

- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices
- All users will be provided with a username and secure password by the ICT Coordinator who will keep an up-to-date record of users. Users are responsible for the security of their username and password
- The ICT Coordinator is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. 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. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes (see appendix for more details). Teachers needing to access a website likely to encounter filtering blocks (e.g. e.g. racism, drugs, discrimination) are to make a specific request to EAC
- Internet filtering/monitoring ensures that children are safe from terrorist and extremist material when accessing the internet
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students etc.)
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement
- Users report any actual/potential technical incident/security breach to the Online Safety Lead (Headteacher) or an Online Safety Coordinator if the headteacher is not available
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up-to-date virus software: SOPHOS
- An agreed process is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems. Supply staff use a supply login giving limited access to school systems to view lesson plans and resources. Trainee teachers have a TGMS device giving more representative access to systems in order for them to fulfil their roles. The guest Wi-Fi is offered to visitors (such as Governors or SEND specialists) allows them to use their devices after reading and abiding by the Visitor Agreement found on the Inventry system when signing in

- An agreed process within the staff AUA is in place regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on school devices that may be used out of school
- An agreed process within the staff AUA is in place that forbids staff from downloading executable files and installing programs on school devices. Users get prompted for an admin username if they try. Staff liaise with the ICT and Communications Coordinator in such circumstances
- TGMS staff do not make use of removable media (e.g. memory sticks/CDs/DVDs) on school devices. Their Google Drive cloud storage is used for data, or their N:Drive on the server

5. Technology

The DfE Filtering and Monitoring Standards states that "Your IT service provider may be a staff technician or an external service provider". The school has an external technology provider (EAC), and it is the responsibility of the school to ensure that the provider carries out all the online safety and security measures that would otherwise be the responsibility of the school. It is also important that the technology provider is fully aware of the school Online Safety Policy/Acceptable Use Agreements and the school has a Data Processing Agreement in place with them.

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school ensures 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.

Filtering & Monitoring

The DFE guidance (for England) on filtering and monitoring in "Keeping Children Safe in Education" states:

"It is essential that governing bodies and proprietors ensure that appropriate filtering and monitoring systems are in place ...governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the … risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified…

The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the

Prevent Duty. To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards…"

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 a governor, in particular when a safeguarding risk is identified or there is a change in working practice

Filtering

- The school manages access to content across its systems for all users and on all devices using the schools 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 Appropriate filtering
- Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- Filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon
- The school has provided enhanced/differentiated user-level filtering allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.

Monitoring

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

- The school monitors all network use across all its devices and services
- Monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored

- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice

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

- Physical monitoring (adult supervision in the classroom)
- Internet use is logged, regularly monitored and reviewed
- Filtering logs are regularly analysed and breaches are reported to senior leaders
- Pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention
- Where possible, school technical staff regularly monitor and record the activity of users on the school technical systems
- Use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)

Mobile Technologies (including BYOD/BYOT)

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

The school has extended mobile technologies to tracking devices, including GPS-enabled smartwatches, mobile phones, and other location-tracking technology. These technologies must follow the same procedures outlined in Appendix 5 for mobile phones.

All users understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The Staff Acceptable Use Policy (Appendix 1) is consistent with and interrelated to other relevant school policies, including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy and this policy. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme, as supported by the Pupil Acceptable Use Agreement (Appendix 2).

The school's Acceptable Use Agreements for staff, pupils/students and parents/carers consider the use of mobile technologies and how devices are used by each stakeholder group. As an overview, the school allows the following:

	School Devices			Personal Devices		
	School owned for single-user	School owned for multiple users	Authorised device	Student owned	Staff owned	Visitor owned
Allowed in school	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*
Full network access (school network)	*Yes*	*Yes*	*Yes*	*N/A*	*Yes*	*No*
Internet only	*N/A*	*N/A*	*N/A*	*N/A*	*Yes*	*Yes*

6. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for 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:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website/social media/local press
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students/pupils in the digital/video images. This requirement is to be reinforced at the start of every school event
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow the school's policies concerning the sharing, distribution and

publication of those images. Those images should only be taken on school/academy equipment; the personal equipment of staff should not be used for such purposes

- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Pupil's work can only be published with the permission of the pupil and parents or carers

7. Data Protection

With effect from 25th May 2018, the Data Protection Arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR). As a result, schools are likely to be subject to greater scrutiny in their care and use of personal data. Schools should ensure that they take account of policies and guidance provided by local authorities or other relevant bodies.

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

The school ensures that:

- It has a Data Protection Policy
- It implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records
- It has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO)
- It has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest
- It has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- The information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- It will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. The school implements a 'Retention Policy' to ensure there are clear

and understood policies and routines for the deletion and disposal of data to support this. Personal data held must be accurate and up to date where this is necessary for the purpose it is processed

- It 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
- Procedures must be in place to deal with the individual rights of the data subject, e.g. One of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them
- Data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring-fenced from systems accessible in the classroom/to learners
- It has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed
- It understands how to share data lawfully and safely with other relevant data controllers
- It reports any relevant breaches to the Information Commissioner within 72 hours of becoming aware of the breach in accordance with UK data protection 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
- As a maintained school, TGMS has a Freedom of Information Policy which sets out how it will deal with FOI requests
- All staff receive data protection training 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
- Where available, tools to monitor the network for Personal Identifying Information (PII) shall be used to ensure that PII is not mishandled

8. Communications

Communication is an area of rapidly developing technologies and uses. The school recognises that a wide range of rapidly developing communications technologies has the potential to

enhance learning. The following table shows how TGMS currently considers the benefits of using these technologies for education to outweigh their risks/disadvantages:

	Staff & other adults				**Students/Pupils**			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school	✓						✓ (Headteacher permission – Appendix 5)	
Use of Tracking Devices in School or on School Trips							✓ (Headteacher permission – Appendix 5)	
Use of mobile phones in lessons			✓ (Headteacher permission)					✓
Use of mobile phones in social time	✓ (In Staff Room or with no pupils present)							✓
Taking photos of pupils on mobile phones				✓				✓
Use of other non-school mobile devices e.g. tablets				✓				✓
Use of personal email addresses in school, or on school network		✓						✓
Use of school email for personal emails				✓				✓
Use of messaging apps		✓						✓
Use of social media		✓ (School X Account)						✓

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils

should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access)

- Users must immediately report (To the Online Safety Lead or Coordinator) the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and students/pupils or parents/carers (e.g. email) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications
- Pupils should be taught about Online Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies. TGMS uses the 'Project Evolve' scheme of learning to provide teachers with the resources they need to meet the government's Internet Safety Strategy of supporting children to stay safe and make a positive contribution online, as well as enabling teachers to develop effective strategies for understanding and handling online risks.

  Within each year group topics include:

  - Self-Image and Identity - This strand explores the differences between online and offline identity beginning with self-awareness, shaping online identities and media influence in propagating stereotypes. It identifies effective routes for reporting and support and explores the impact of online technologies on self-image and behaviour
  - Online Relationships - This strand explores how technology shapes communication styles and identifies strategies for positive relationships in online communities. It offers opportunities to discuss relationships, respecting, giving and denying consent and behaviours that may lead to harm and how positive online interaction can empower and amplify voice
  - Online Reputation - This strand explores the concept of reputation and how others may use online information to make judgements. It offers opportunities to develop strategies to manage personal digital content effectively and capitalise on technology's capacity to create effective positive profiles
  - Online Bullying - This strand explores bullying and other online aggression and how technology impacts those issues. It offers strategies for effective reporting and intervention and considers how bullying and other aggressive behaviour relates to legislation
  - Managing Online information - This strand explores how online information is found, viewed and interpreted. It offers strategies for effective searching, critical evaluation of data, the recognition of risks and the management of online threats and challenges. It explores how online threats can pose risks to

our physical safety as well as online safety. It also covers learning relevant to ethical publishing

- Privacy and Security - This strand explores how personal online information can be used, stored, processed and shared. It offers both behavioural and technical strategies to limit impact on privacy and protect data and systems against compromise
- Copyright and Ownership - This strand explores the concept of ownership of online content. It explores strategies for protecting personal content and crediting the rights of others as well as addressing potential consequences of illegal access, download and distribution

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

9. Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. They could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

TGMS provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions

School staff should ensure that:

- No reference should be made in social media to students, parents/carers or school staff
- They do not engage in online discussions on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise the risk of loss of personal information

When official school social media accounts are established, there should be:

- A process for approval by senior leaders

- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
    - 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 that associates itself with the school or impacts 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 the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to proactively 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
- The school's use of social media for professional purposes will be checked regularly by the Online Safety Group to ensure compliance with the school policies

10. Dealing with unsuitable/inappropriate activities

TGMS believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 TGMS would refer to updated guidance about dealing with self-generated images/sexting as highlighted in – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) Serious or repeat offences would be reported to the police. Under the Cyber-Prevent agenda, the National Crime Agency has a remit to prevent young people becoming involved in cyber-crime and harness their activity in positive ways – further information here						X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school, unless agreed with the school's Leadership Team.					X	

Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
Unfair usage (downloading/uploading large files that hinder others in their use of the internet)				X	
Using school systems to run a private business				X	
Intentional infringement of copyright				X	
Online gaming				X	
Online gambling				X	
Online shopping/commerce		X			
File sharing		X			
Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting e.g. YouTube		X			

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

If there is any suspicion that the website (s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (Appendix 3), responding to online safety incidents and report immediately to the police.

Other Incidents

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

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported
- Conduct the procedure using a designated computer that will not be used by young people, and if necessary, can be taken off-site by the police should the need arise. Use the same computer for the duration of the procedure
- It is important to ensure that the relevant staff 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
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national/local organisation (as relevant)
    - Police involvement and/or action
- If the content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - Incidents of 'grooming' behaviour
    - The sending of obscene materials to a child
    - Adult material which potentially breaches the obscene publications act
    - Criminally racist material
    - Promotion of terrorism or extremism
    - Offences under the computer misuse act (see user actions chart above)
    - Other criminal conduct, activity or materials
    - Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation

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

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Pupil Incidents	Refer to class teacher	Refer to Headteacher (or SLT)	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X		X		
Unauthorised use of non-educational sites during lessons							X
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device		X			X		X
Unauthorised / inappropriate use of social media / messaging apps / personal email		X			X		X
Unauthorised downloading or uploading of files		X			X		X
Allowing others to access the school network by sharing username and passwords		X			X		
Attempting to access or accessing the school network, using another student's / pupil's account		X			X		
Attempting to access or accessing the school network, using the account of a member of staff		X			X		
Corrupting or destroying the data of other users		X			X		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X			X		X (LA)
Continued infringements of the above, following previous warnings or sanctions		X	X		X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X			X		X
Using proxy sites or other means to subvert the school's filtering system		X			X		X

Accidentally accessing offensive or pornographic material and failing to report the incident		X			X		X
Deliberately accessing or trying to access offensive or pornographic material		X			X		
Receipt or transmission of material that deliberately infringes the copyright of another person or infringes the Data Protection Act		X			X		X

	Actions/Sanctions						
Staff Incidents	**Refer to line manager**	**Refer to Headteacher**	**Refer to Local Authority (LADO)**	**Refer to Police**	**Refer to Technical Support Staff for action re filtering etc.**	**Warning**	**Disciplinary action**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X			
Inappropriate personal use of the internet / social media / personal email		X				X	
Unauthorised downloading or uploading of files		X				X	
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X					
Careless use of personal data e.g. holding or transferring data in an insecure manner		X					
Deliberate actions to breach data protection or network security rules		X				X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X				X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X				X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X				X	X
Actions which could compromise the staff member's professional standing		X				X	X
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy		X				X	X

Using proxy sites or other means to subvert the school's / academy's filtering system		X				X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X				X	
Deliberately accessing or trying to access offensive or pornographic material		X				X	X
Breaching copyright or licensing regulations		X				X	
Continued infringements of the above, following previous warnings or sanctions		X				X	X

Appendices

Appendix 1: Staff Acceptable Use Policy

	Name of School	**Tylers Green Middle School**
	AUP review Date	**Autumn 2025**
	Date of next Review	**Autumn 2027**
	Who reviewed this AUP?	**S Isaacs/C Johnson**

Acceptable Use Policy (AUP): Staff agreement form

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business.
  (This is currently…….@tylersgreenmiddle.co.uk)
- I will only use the approved school email, school Learning Platform or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet.
- I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff and will not store images at home.
- I will use the school's Learning Platform in accordance with school protocols.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to as per the school's Code of Conduct.
- I agree and accept that any computer, laptop or tablet loaned to me by the school is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will access school resources remotely (such as from home) only through the school-approved methods.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption outside of the school email network.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential,

EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

- I will embed the school's e-safety curriculum into my teaching.
- I will alert the school's named DSL / relevant senior member of staff if I feel the behaviour of any child I teach may be a cause for concern.
- I understand that all Internet usage / and network usage can be logged, and this information could be made available to my manager on request.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff / named DSL at the school.
- I understand that if hardware loaned from the school is lost, stolen or damaged, I will report this to the School Business Manager immediately.
- All iPads must have 'lost mode' enabled so that individual iPads can be traced.
- When required, all computers, laptops and tablets should be returned to school, for instance, when requiring an update.
- I will use the technology provided by the school in line with the school's policies:
    - GDPR; Staff Privacy Policy
    - Staff GDPR Procedures
    - Staff Code of Conduct.
- Use of iPads will be in line with the guidance supplied by Apple: Apple School Manager Agreement.
- I understand that failure to comply with this agreement could lead to disciplinary action.

Acceptable Use Policy (AUP): Staff agreement form

User Signature:

- I agree to abide by all the points above.
- I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.
- I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

Signature .....Date.....

Full Name ..... (printed)

Job title .....

School .....

Authorised Signature
Mr S Isaacs
Head teacher

I approve this user to be set up.

Signature ..... Date .....

Full Name ..... (printed)

Appendix 2: Pupil Acceptable Use Agreement

TYLERS GREEN MIDDLE SCHOOL

KS2 Pupil Acceptable Use Agreement

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will treat the school's computer equipment carefully and with respect.
- I will never try to download, install or remove software/applications onto or from the school computers.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I will not bring USB sticks into school, any file to be brought into school will be sent via email to the school office or on my Google Classroom.
- I am aware that some websites and social networks have age restrictions, and I should respect this.
- I will not attempt to visit internet sites that are not appropriate to children of my age or that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- I will think carefully about the messages I send (including the use of social media), or information I upload, and be polite and sensible, as I may unintentionally hurt the feelings of other people.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will also not share personal information about others on the internet.
- I will never arrange to meet someone I have only ever previously met on the internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.
- If I receive an inappropriate image, I will delete it immediately and then report it to a teacher / responsible adult.
- When taking photos, these will only be saved to the approved school account.
- I will only use digital technology under the instruction of the adults in school, not for personal or unsupervised activities.
- I understand that according to the Education Act 2011, the school has the right to search my electronic devices brought into school and the right to delete data if there is a breach of online safety rules.

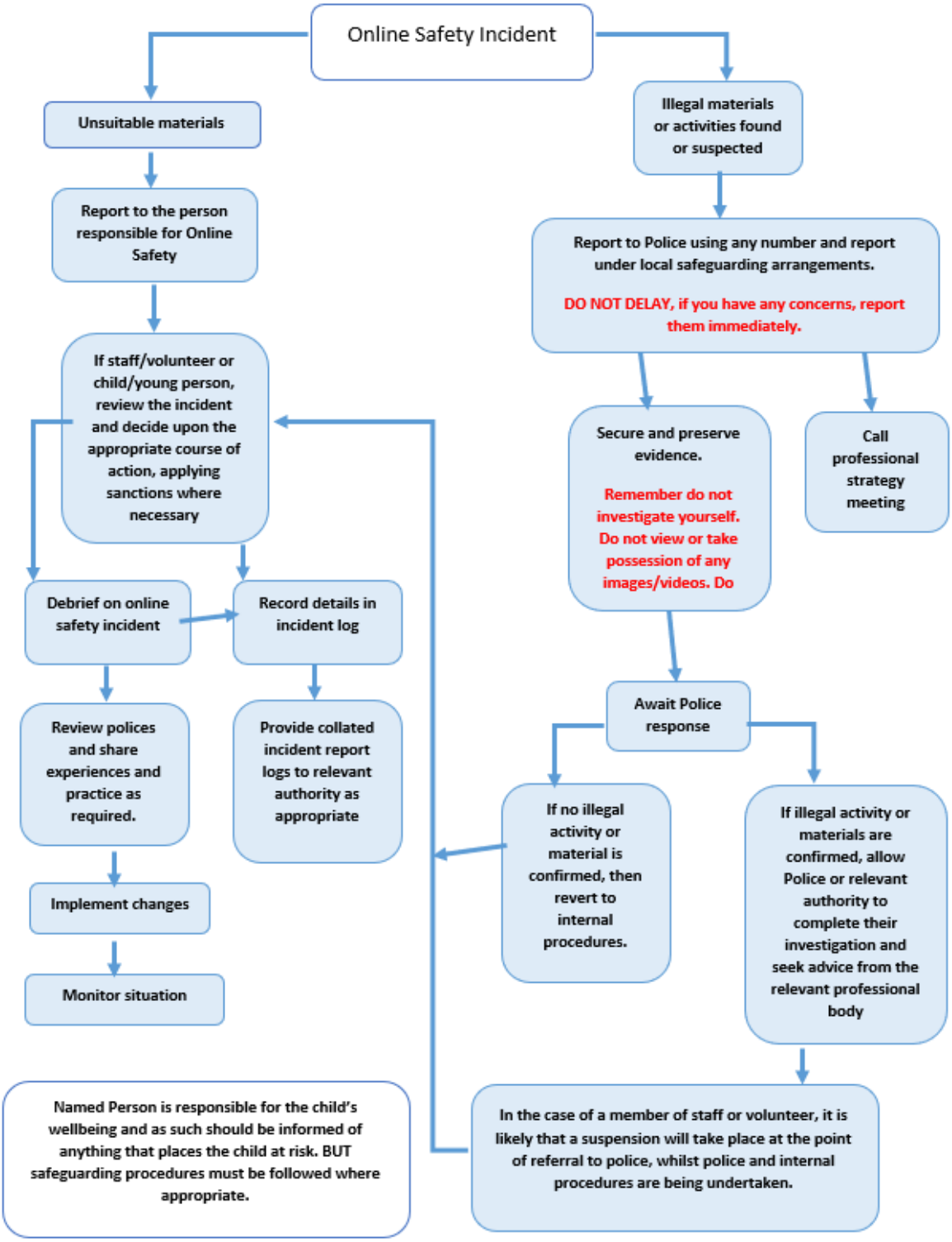
This will be discussed and signed by the pupils in class – please keep this for your reference.

Name: _____

Signed: _____

Date: _____

Appendix 3: Responding to incidents of misuse flowchart



Appendix 4: School's Response to KCSIE 2023 Filtering and Monitoring Requirements

The Department of Education Keeping Children Safe in Education (KCSIE) 2023 Statutory Guidance firmly puts the responsibility for the provision and operation of web filtering and monitoring solutions on school leadership rather than on the IT team.

- School governing bodies and proprietors have overall strategic responsibility for filtering and monitoring.
- SLTs are responsible for procuring filtering and monitoring systems, documenting decisions on what is blocked or allowed and why, reviewing the effectiveness of filtering provision, and overseeing reports.
- SLTs and DSLs have a responsibility to understand filtering and monitoring systems.

Securly's Securly's Safety and Wellness ecosystem makes Filtering and Monitoring Compliance easy.

With cloud based web filtering and monitoring powered by its market leading AI, Securly prevents access to inappropriate websites, provides alerts on detected student safety issues, monitors student wellness levels, and allows teachers to monitor student activity on devices in class. Throughout the solution there is focus on minimising staff workload whilst identifying at risk students and enabling early intervention.

For more information, or a product demonstration, please contact us:

01844 21 50 50

eac-ns.co.uk

EAC | OUTSTANDING IT INTEGRATION

Built for Education, Designed for Schools.	Securly's suite of solutions is built for and sold exclusively to schools. These intuitive and easy-to-use products are designed for use by teaching staff and DSLs.
Delegated Administration	Securly's delegated administration options give teaching staff direct access to web filter policy management, alerts, and wellness dashboard data. Securly Filter and Aware are configurable to ensure staff only receive access to information on students that they are responsible for, reducing unnecessary work and keeping data secure.
Filtering and Monitoring Any Device Anywhere	Securly's cloud architecture supports all device types (Windows, Chrome, iOS, MAC, Android, etc.) in all locations (in school and away from school). It supports school-owned devices, guest networks, and BYOD.
Student Safety Alerts	Securly Aware uses the industry's longest-learning AI to examine student internet activity across searches, social media, web browsing, email, chat, and shared documents. It identifies potential issues such as bullying, violence, self-harm, grief, and suicide and notifies DSLs instantly.
Monitoring Wellness Levels	Securly Aware conducts a real-time analysis of student activity to understand if they're showing signs of distress and assigns a reliable, real-time wellness level. Wellness level scores provide a simple indication of an individual students' state of mind and direction of change, enabling DSLs to understand which students require immediate intervention.
Monitoring Devices	Securly Classroom provides cloud-based classroom management, enabling teachers to see student screens in a class session. This helps teachers guide lessons, monitor student progress, and keeps the focus on learning.

Any automated alert system has the potential to deliver too many alerts and false positives. Securly's AI and configuration options minimise false positives and reduce staff workload.

Minimising Staff Workload

By examining whole sentences rather than key words and using "sentiment analysis" to identify negative context, Securly minimises false positives. The alert triggers can also be customised for different groups of students, increasing or decreasing the level at which an alert is triggered.

Outsourcing Alert Monitoring and Investigation with On-Call

Schools rely on On-Call to help identify and respond to students at risk of self-harm, suicide, bullying, and violence. The On-Call Team analyses alerts from Securly Aware and notifies school staff immediately to ensure that alerts are followed up in the shortest possible timescale, leaving teachers free to teach!

For more information, or a product demonstration, please contact us:

01844 21 50 50

eac-ns.co.uk

EAC | OUTSTANDING IT INTEGRATION

How Securly Helps Schools

Meet KCSIE Filtering Guidance

securly

Securly Filter is a web filter designed for schools and widely deployed in the UK and around the world. As UK government guidance evolves Securly makes every effort to ensure that its products comply and help schools comply with their statutory obligations around student safety and well-being.

filter

Securly Filter is one of a suite of school focused safety products from Securly designed to make it seamless for schools to meet their student safety obligations. Specifically, Securly Filter meets the filtering technical requirements, and Securly Aware and Securly Classroom help schools meet their KCSIE monitoring obligations.

Responses to KCSIE Web Filter Requirements

Make sure your filtering provider is:

KCSIE GUIDANCE	SECURLY RESPONSE
A member of Internet Watch Foundation (IWF).	Securly has been an IWF member since 01/03/2016.
Signed up to Counter-Terrorism Internet Referral Unit list (CTIRU).	Securly receives and incorporates the CTIRU feed into its filtering technology.
Blocking access to illegal content including child sexual abuse material (CSAM).	Securly blocks access to illegal content including CSAM.
If the filtering provision is procured with a broadband service, make sure it meets the needs of your school or college.	Securly works with broadband providers and managed service providers to ensure Securly Filter is well configured and fit for purpose.

Your filtering system should be operational, up to date and applied to all:

KCSIE GUIDANCE	SECURLY RESPONSE
Users, including guest accounts.	Securly Filter can be applied to all device types and all user categories in all locations, with user-level logging and filtering through sign-in and directory integration with Microsoft Azure or Google G-Suite. Securly's cloud architecture supports all device types (Windows, Chrome, iOS, MAC, Android, etc.) in all locations (in and away from school). It supports school-owned devices, guest networks, and BYOD.
School-owned devices.	Securly Filter can be applied to the school network, filtering all devices on the network and to individual school owned devices, of all types, including but not limited to windows, chrome, iOS, Android, Linux. School owned devices can then be filtered in any location.
Devices using the school broadband connection.	Securly Filter can also be applied to BYOD devices, and Guest networks ensuring all devices using the school broadband connection are appropriately filtered.

Your filtering system should:

KCSIE GUIDANCE	SECURLY RESPONSE
Filter all internet feeds, including any backup connections.	Securly Filter can be applied at both the user/device level and at the network level.
Be age and ability appropriate for the users, and be suitable for educational settings.	Securly Filter is built exclusively for education and has school appropriate filtering configured out-of-the-box with simple configuration of more strict or relaxed policies as required. Through manual configuration or directory integration age appropriate (and other group) settings may be implemented.
Handle multilingual web content, images, common misspellings and abbreviations.	Securly Filter and it's classification engine PageScan (incorporation text scan and image scan) use dynamic categorisation, crowd sourced URL scanning, search engine crawling and paid 3rd party categorisation to keep its classification database up to date and to dynamically categorise new sites. This is an industry standard approach which covers text and images, is multilingual and handles common abbreviations and misspellings.
Identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them.	Securly works with schools to ensure Securly Filter is applied in the most robust way possible and includes publicly available best practice guides and recommendations for configuring devices and networks to best protect children and prevent circumvention.
Provide alerts when any web content has been blocked.	Securly Filter includes the ability to generate instant alerts for blocked content, this is configurable at a policy level to allow for different alert levels for vulnerable users.
Mobile and app content is often presented in a different way to web browser content. If your users access content in this way, you should get confirmation from your provider as to whether they can provide filtering on mobile or app technologies. A technical monitoring system should be applied to devices using mobile or app content to reduce the risk of harm.	Securly Aware connects directly into Microsoft Office365 and G-Suite Workspace to scan documents, emails, chats, images, and videos for inappropriate content regardless of where those systems are used or how they are accessed.
It is important to be able to identify individuals who might be trying to access unsuitable or illegal material so they can be supported by appropriate staff, such as the senior leadership team or the designated safeguarding lead.	Securly Filter categorises blocked URLs in a way designed to be useful in schools, Categories include pornography, drugs, gambling, hate and other adult. Students trying to access unsuitable material will be blocked, an alert is generated and the activity logged against the student. Appropriate staff may investigate via the reporting system.

Your filtering systems should allow you to identify:

KCSIE GUIDANCE	SECURLY RESPONSE
Device name or ID, IP address, and where possible, the individual.	Securly Filter logs the username from Microsoft Azure AD or G-Suite; for shared devices, a device name or serial number may be used instead, or where authentication is not possible, an IP address is recorded. This information determines if a device or user is on-site or off-site and if policies should differ based on that measure.
The time and date of attempted access.	The search term or content being blocked by Securly Filter and Securly Aware is logged and includes a date and timestamp for all activities.
The search term or content being blocked.	Securly Filter logs search terms in a format that is easy for non-technical users to inspect and understand.

Appendix 5: REQUEST FOR PERMISSION TO BRING A MOBILE PHONE / SMART DEVICE WITH A SIM TO SCHOOL

Note: From September 2026, TGMS will not permit smartphones to be brought onto the school site by pupils, including for storage or hand-in, except in the most exceptional circumstances where a smartphone forms an essential part of a pupil's medical care or safeguarding plan, and only with explicit written permission from the Headteacher.

REQUEST FOR PERMISSION TO BRING A MOBILE PHONE, SMART DEVICE WITH A SIM OR MOBILE TECHNOLOGY WITH LOCATION-TRACKING CAPABILITY

To: Mr Isaacs, Headteacher, Tylers Green Middle School

Pupil Name: …… **Class: …….**

I wish to apply for permission for my child to bring his/her mobile phone / smart device with SIM / mobile technology with location-tracking capability (*please delete as appropriate)* to school. The device is required for the following reasons:

Pupils who bring a mobile phone/smart device with SIM/mobile technology with location-tracking capability to school must abide by the school's policy on the use of mobile phones and technologies, which states that:

2.6. Mobile Phone Safety: *Individual pupils are only permitted to have mobile phones in school with the agreement of the head teacher. Mobile phones must be handed into the office on arrival at school and collected at the end of the day. Pupils are not permitted to carry mobile phones at any time during the school day.*

2.7. Other New/Mobile Technologies Safety: *This is a fast-developing landscape where new technologies, such as wearable devices and mobile technology with location-tracking capability, are being rapidly introduced to the market. The same principles will apply to mobile phones unless express permission is given for them.*

Please note that although phones/devices will be kept in the school office during the day, bringing them into school is done so at your own risk. The school also reserves the right to revoke permission if pupils do not abide by the policy.

Signed: …….. Date: …… (Parent/Guardian)

Parent/Guardian name (block capitals): ……

---

*To be completed and returned by Headteacher

To: ……

PERMISSION TO BRING A MOBILE PHONE/SMART DEVICE WITH SIM/MOBILE TECHNOLOGY WITH LOCATION-TRACKING CAPABILITY INTO SCHOOL

Pupil name: …….. Class: ……

I confirm that permission has/has not been granted for your child to bring their mobile phone/smart device in to school. Please note that any mobile phone/device is brought in to school at the owner's risk and it must be handed in at the School Office and collected at the end of the day.

The phone/device must be labelled and switched off.

Signed: …… Date: ……

Mr S Isaacs, Ba (Hons), Ma (Ed)

Appendix 6: Guiding Digital Childhoods (GDC) Addendum

Purpose

This appendix sets out Tylers Green Middle School's commitment to the Guiding Digital Childhoods (GDC) initiative, developed collaboratively across the Chiltern Area Partnership (CAP). The GDC programme aims to support children and families to establish healthy digital habits, balance online and offline life, and reduce the pressures associated with early smartphone and social media use.

This work complements (and does not replace) statutory online safety responsibilities under KCSIE, DfE Online Safety Guidance (2023), the Education Act 2002, and Ofsted's emphasis on digital safeguarding and childhood development.

Context and Rationale

Research, including Jonathan Haidt's *The Anxious Generation* (2024), highlights significant developmental and mental-health risks associated with early smartphone and social media exposure, including impacts on sleep, anxiety, resilience and social interaction.

A CAP-wide parent survey (2024–25), representing over 3,000 pupils aged 4–17, showed strong community support for:

- Delaying smartphone access
- Delaying social media use
- Prioritising face-to-face friendships and real-world play
- Schools supporting parents to feel confident about boundary-setting

Parents also reported feeling peer pressure and isolation in making these decisions individually, highlighting the need for a collective, community-based response.

Guiding Principles for Families

As a CAP school, we advocate for and support families to adopt the following developmental principles:

- **Delay smartphones until at least Year 9**
- **Delay social media until age 16**
- **Keep school time phone-free**
- **Prioritise real-world independence, free play and social development**

School Commitments

To model and reinforce these principles, Tylers Green Middle School commits to:

- Maintaining a **phone-free school day** for pupils
- **Actively teaching digital safety, literacy, mindfulness and responsibility**
- Providing **clear, supportive information and workshops** for families
- **Modelling healthy tech use** as a staff body and promoting balance and intention in digital interactions

These commitments align with Ofsted's emphasis on education for character, resilience, mental health, and safe online behaviours.

Support for Parents & Community Action

To reduce social pressure and enable collective confidence, the school will:

- Provide evidence-based digital well-being guidance
- Host parent information sessions and workshops
- Participate in the CAP **voluntary pledge and register** for families wishing to delay smartphones and social media
- Develop a dedicated **GDC area on our school website** with resources and advice
- Explore partnerships with local organisations and community groups to promote real-world play and digital balance

Participation in the voluntary register is optional and anonymous.

Pupil Involvement

We will involve pupils where developmentally appropriate, including:

- Pupil-voice contributions to resources
- Peer-to-peer guidance (e.g. older year groups supporting younger pupils)
- Celebrating offline achievements and independence

Review and Monitoring

This addendum will be:

- Reviewed annually alongside the Online Safety Policy
- Informed by the CAP GDC sub-committee
- Updated in line with emerging research and national guidance