Online Safety Policy
Whole School Policy including EYFS

TPS aspires for each child to thrive personally, socially and academically by creating an inclusive environment that promotes wellbeing, encourages curiosity and celebrates individual success.

Date Revised:	March 2024
Approval Body:	Board of Governors
Date Approved:	April 2024
Review Schedule:	Annually
Circulation:	Governors, all staff, parents, pupils, volunteers

Contents

1. **Scope**

   This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors) 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 School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

2. **Objectives**

   The School's 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 pupils 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 e.g. reference drive (R)
   - is published on the school website.

3. **Roles & 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.

   3.1. **Board of Governors**

   Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the UKCIS document "Online Safety in Schools and Colleges – questions from the Governing Body".

   This review will be carried out by the Education Committee whose members will receive regular information about online safety incidents and monitoring reports.

   A member of the governing body will take on the role of Online Safety Governor to include:

- regular meetings with the DSL and Online Safety Co-ordinator
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually
- reporting to the full Board of Governors
- receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards
- 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.

3.2. Headmaster and Senior Leadership Team (SLT)
The Headmaster:
- has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead (DSL), as defined in Keeping Children Safe in Education
- and the Deputy Head are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff
- is responsible for ensuring that the DSL, Online Safety Co-ordinator, Network Consultant and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant
- 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
- and Senior Leadership Team (SLT) will receive regular monitoring reports from the DSL and Online Safety Co-ordinator
- will work with the responsible Governor, DSL, Online Safety Co-ordinator and Network Consultant in all aspects of filtering and monitoring.

3.3. Designated Safety Lead (DSL)
The DSL will:
- hold the lead responsibility for online safety, within their safeguarding role
- 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
- meet regularly with the Online Safety 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
- attend relevant governing body meetings/groups
- report regularly to the Headmaster and SLT
- 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

- liaise with staff and the Network Consultant on matters of safety and safeguarding and welfare (including online and digital safety)
- The Online Safety Co-ordinator works in support of the DSL in carrying out these responsibilities.

3.4. Online Safety Co-ordinator

The role of the Online Safety Co-ordinator is undertaken by the Head of ICT & Computing. The Online Safety Co-ordinator:

- will be a member of the Online Safety Group
- work closely on a day-to-day basis with the DSL
- 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
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the School and beyond
- liaise with Heads of Departments to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- 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
- provide (or identify sources of) training and advice for staff, governors, parents and pupils
- liaise with the School, Local Authority, Network Consultant, pastoral staff and support staff (as relevant)
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by pupils) with regard to the areas defined In Keeping Children Safe in Education:
    - content
    - contact
    - conduct
    - commerce.

3.5. Online Safety Group

The Online Safety Group has the following members:
- Headmaster
- Designated Safeguarding Lead
- Online Safety Co-ordinator
- Online Safety Governor
- Network Consultant

Members of the Online Safety Group will assist the DSL with:
- the production, review and monitoring of the school's Online Safety Policy
- the production, review and monitoring of the school's filtering policy and requests for filtering changes
- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage
- reviewing network, filtering, monitoring and incident logs, where possible

- encouraging the contribution of staff awareness to emerging trends and the school's online safety provision
- consulting stakeholders – including staff, parents/carers about the online safety provision
- monitoring improvement actions identified through review processes.

3.6. Network Consultant

The Network Consultant (Brandtek Ltd) is responsible for ensuring:
- they are aware of and follow the school Online Safety Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from Local Authority or other relevant body
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the DSL for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- monitoring systems are implemented and regularly updated as agreed in school policies.

3.7. Teaching and Support Staff

School staff are responsible for ensuring that:
- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the Acceptable Use of I.T. Agreement
- they immediately report any suspected misuse or problem to the DSL for investigation/action, in line with the school safeguarding procedures
- all digital communications with pupils and parents are on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and Acceptable Use Agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

3.8. Pupils
- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement and Online Safety Policy
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology.
- should 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.

3.9. Parents and Carers
The School will take every opportunity to help parents and carers understand these issues through:
- publishing the school Online Safety Policy on the school website
- providing them with access to the pupils' Acceptable Use agreement (on My School Portal)
- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images
- parents' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the School in:
- reinforcing the online safety messages provided to pupils in school.
- the safe and responsible use of their children's personal devices in the School (where this is allowed).
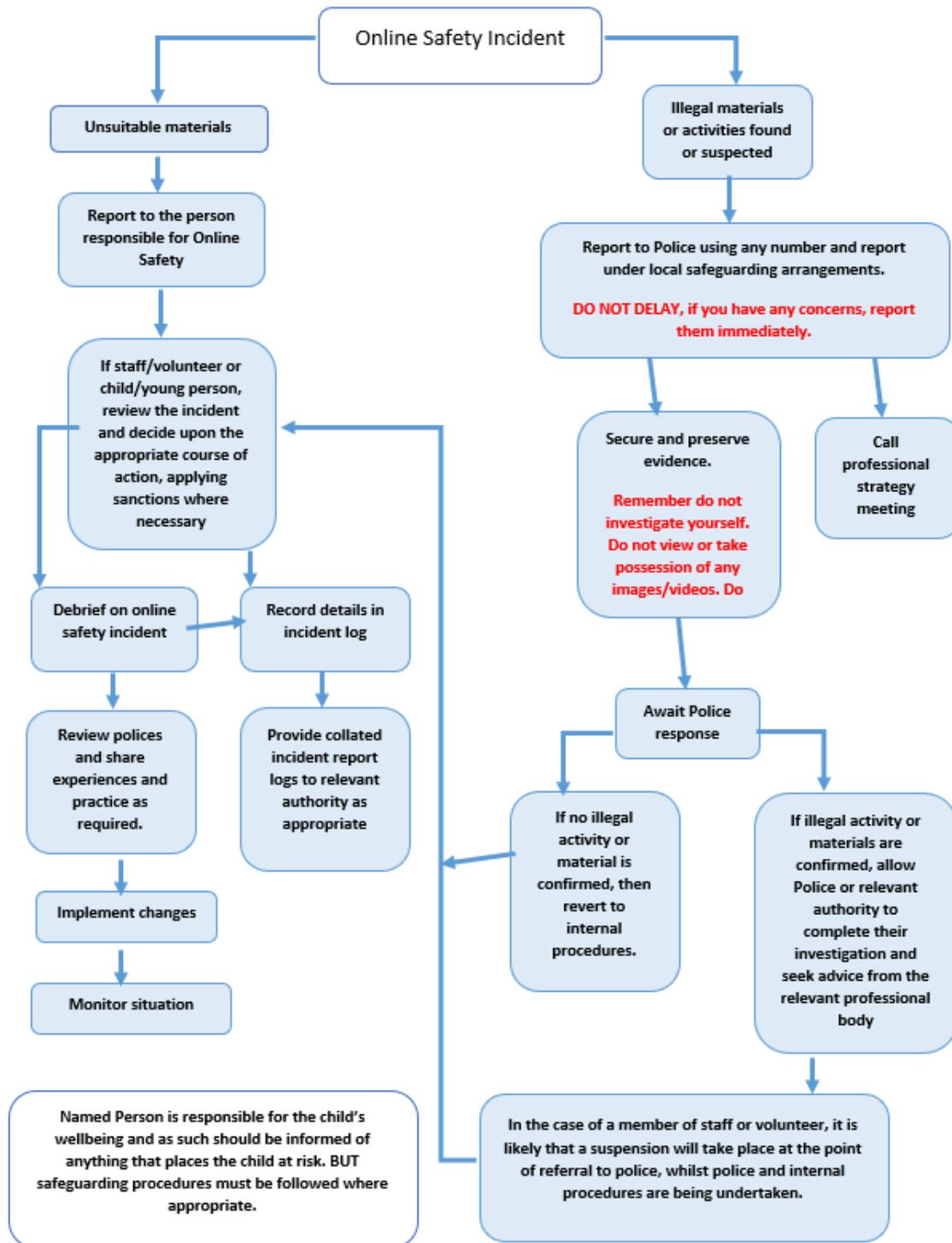
4. Reporting & Responding
The School will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the School) which will need intervention. The School will ensure:
- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Co-ordinator and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm, the incident must be escalated through the agreed school safeguarding procedures, this may include:
  - non-consensual images
  - self-generated images
  - terrorism/extremism
  - hate crime/ abuse

- o fraud and extortion
- o harassment/stalking
- o child sexual abuse material (CSAM)
- o child sexual exploitation grooming
- o extreme pornography
- o sale of illegal materials/substances
- o cyber or hacking offences under the computer misuse act
- o copyright theft or piracy.

- any concern about staff misuse will be reported to the Headmaster, unless the concern involves the Headmaster, in which case the complaint is referred to the Chair of Governors and the local authority
- 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:
    - o internal response or discipline procedures
    - o involvement by local authority
    - o police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively

Responding to Online Safety Incidents


```
                            Online Safety Incident
```

Unsuitable materials
↓
Report to the person responsible for Online Safety
↓
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
↓
Debrief on online safety incident → Record details in incident log
↓
Review polices and share experiences and practice as required.
↓
Implement changes
↓
Monitor situation

Provide collated incident report logs to relevant authority as appropriate

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

Illegal materials or activities found or suspected
↓
Report to Police using any number 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 view or take possession of any images/videos. Do

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

The Designated Safety Lead (DSL) at TPS is the individual responsible for Online Safety
CEOP: Child Exploitation and Online Protection Centre
CEOP is a law enforcement agency whose aim is to help keep children and young people safe from sexual abuse and grooming online.

5. **School Actions**

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

6. **Online Safety Education Programme**

   6.1. **Pupils**

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

   - a planned online safety curriculum for all year groups matched against a nationally agreed framework and regularly taught in a variety of contexts.
   - lessons are matched to need; are age-related and build on prior learning
   - lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
   - pupils' needs and progress are addressed through effective planning and assessment
   - digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE and ICT
   - the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language
   - vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND
   - acceptable use is reinforced across the curriculum
   - 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, learners are guided to sites checked as suitable for their use and processes 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 are vigilant in supervising and monitoring the content of the websites visited
   - 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 the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
   - the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

   6.2. **Parents and Carers**

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

   - regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes

- regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc
- the pupils – who are encouraged to pass on to parents the online safety messages they have learned in lessons
- letters, newsletters and website
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant web sites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers

6.3. The Wider Community

The School will provide opportunities for members of the school's community to gain from the School's online safety knowledge and experience. This may be offered through the following:
- providing family learning events in use of new digital technologies, digital literacy and online safety
- online safety messages targeted towards grandparents and other relatives as well as parents
- providing online safety information via the schools website and social media

6.4. Staff and Volunteers

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 and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school's Online Safety Policy and Acceptable Use Agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
- the DSL and Online Safety Co-ordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations
- this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- the DSL and Online Safety Co-ordinator (or other nominated person) will provide advice/guidance/training to individuals as required.

6.5. Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety and safeguarding. This may be offered in several ways such as:
- attendance at relevant training
- participation in school training / information sessions for staff or parents (this may include attendance at assemblies/lessons).

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

7. Technology

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

8. Filtering & Monitoring

The School's filtering and monitoring provision is agreed by the SLT, DSL, Online Safety Co-ordinator, and Governors (with the involvement of the Network Consultant). It 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 Network Consultant will have technical responsibility.

Checks on the filtering and monitoring system are carried out by the Network Consultant with the involvement of the Online Safety Co-ordinator, DSL and the Online Safety Governor, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced .

8.1. 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
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes
- filtering logs are regularly reviewed and alert the Online Safety Co-ordinator to breaches of the filtering policy, which are then acted upon.

8.2. 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 Online Safety Co-ordinator and the DSL, 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 management
- 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

9. **Technical Security**

The School technical systems are managed in ways that ensure that the School meets recommended technical requirements:
- responsibility for technical security resides with SLT who may delegate activities to identified roles.
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT Network Consultant and will be reviewed, at least annually, by the Online Safety Group
- password policy and procedures are implemented.
- all users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- all school networks and systems will be protected by secure passwords. Passwords must not be shared with anyone.
- the administrator passwords for school systems are kept in a secure place.
- there is a risk-based approach to the allocation of learner usernames and passwords.
- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- appropriate security measures are in place (schools may wish to provide more detail which may need to be provided by the service provider) to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- the Network Consultant is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person.

- use of school devices out of school is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network
- staff members are not permitted to install software on a school-owned devices
- removable media is not permitted unless approved by the SLT
- systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- mobile device security and management procedures are in place (where mobile devices are allowed access to school systems).
- guest users are provided with appropriate access to school systems based on an identified risk profile.

10. Mobile Technologies

The School provides tablets to staff if a requirement of their role. Staff should understand that the primary purpose of the tablet is educational and that their use should be consistent with the I.T. Acceptable Use Policy. No personal apps or personal information should be installed on school mobile technologies and the device is for the **sole** use of the staff member. Staff are responsible for the safety and care of the tablet provided. The School reserves the right to charge staff members for repairs/replacements if damages are due to negligence.

Tablets may be provided to pupils during lessons for educational purposes. Pupils are not permitted to use personal mobile technologies during school hours, without prior authorisation from the Headmaster.

School owned/provided devices:

- all school devices are managed though the use of Mobile Device Management software
- there is an asset log that clearly states whom a device has been allocated to. There is clear guidance on where, when and how use is allowed
- the use of devices on trips/events away from school is clearly defined and expectations are well-communicated.
- liability for damage aligns with current school policy for the replacement of equipment.
- education is in place to support responsible use.

Personal devices:

- there is a clear policy covering the use of personal mobile devices on school premises for all users
- where devices are used to support learning, staff have been trained in their planning, use and implementation, ensuring that all learners can access a required resource.
- use of personal devices for school business is defined in the Acceptable Use Agreement. Personal devices commissioned onto the school network are segregated effectively from school-owned systems
- the expectations for taking/storing/using images/video aligns with the school's Acceptable Use Agreement and Digital Image Guidelines. The non-consensual taking/using of images of others is not permitted.

- education about the safe and responsible use of mobile devices is included in the school online safety education programmes

Pupils in Reception – Year 5 are not permitted to bring mobile phones to School. Pupils in Year 6 - 8 may bring a mobile phone to School if required for travel arrangements. All phones must be stored in the School Office during school hours.

11. Social Media

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

- ensuring that personal information is not published.
- education/training being provided
- clear reporting guidance, including responsibilities, procedures, and sanctions.
- risk assessment, including legal risk.
- guidance for pupils and parents/carers

School staff should ensure that:

- no reference should be made in social media to pupils, parents/carers or school staff.
- they do not engage in online discussion on personal matters relating to members of the school community.
- personal opinions should not be 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, there should be:

- a process for approval by the Headmaster
- 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.

12. Digital and Video Images

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

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- when using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images.
- staff/volunteers are aware of those pupils 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 children at school events for their own personal use (as such use in 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 pupils in the digital/video images
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that pupils are appropriately dressed
- pupils must not take, use, share, publish or distribute images of others without their permission within the school environment
- photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with Online Safety Policy
- pupils' full names will not be used anywhere on a website or in editorial content, particularly in association with photographs, unless permission is given.
- permission from parents or carers will be obtained in advance regarding use of digital images. Permission is not required for images taken solely for internal purposes
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- images will be securely stored in line with the school's Data Retention & Storage Policy

Further detail can be found in the School's Guidelines for Taking and Using Images of Pupils that is located on the school's website.

13. Online Publishing

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

- Public-facing website
- Social media
- Weekly newsletters bulletin

The school website is managed/hosted by an external provider. 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 magazines and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where pupil work, images or videos are published, their identities are protected, and full names are not published, unless permission has been granted.

The school public online publishing provides information about online safety e.g., publishing the school's Online Safety Policy, curating latest advice and guidance; news articles etc, through the School bulletin and MSP.

These include reference to an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process.

14. Data Protection

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

For further information the following documents are available on the Reference Drive (R):

- Data Protection Policy
- Privacy Notices (Staff, Pupil and Parent)
- Data Retention & Storage Policy.