



WATTON WESTFIELD  
INFANT & NURSERY

---

WATTON JUNIOR

## Online safety policy

This policy will be reviewed in full by the Governing Body on an annual basis.

Reviewed By	LGB
Meeting at which policy was reviewed and approved	November 2025
Next Review Date	November 2026

## Contents

1.0	Scope of the Online Safety Policy .....	2
2.0	Process for monitoring the impact of the Online Safety Policy .....	2
3.0	Policy Aims .....	2
4.0	Policy and leadership .....	3
5.0	Responding to online safety incidents .....	9
6.0	Filtering & Monitoring .....	11
7.0	Technical Security .....	13
8.0	Online Publishing .....	14
9.0	Cyber Security .....	15
10.0	Related policies .....	15

### 1.0 Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Watton Westfield & Watton Junior Schools to safeguard members of our school community online in accordance with statutory guidance and best practice.

**This Online Safety Policy applies to all members of the school community (including staff, pupils, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).**

Watton Westfield & Watton Junior Schools 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.

### 2.0 Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- *logs of reported incidents*
- *Filtering and monitoring logs*
- *internal monitoring data for network activity*
- *surveys/questionnaires of:*
  - *pupils*
  - *parents and carers*
  - *staff.*

### 3.0 Policy Aims

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication

- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard pupils in the digital world
- describes how the school will help prepare pupils 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 the schools' SharePoint pages.
- *is published on the school website.*

## 4.0 Policy and leadership

### 4.1 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.

### 4.2 Executive Headteacher and senior leadership team

- The Executive Headteacher 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, as defined in Keeping Children Safe in Education.
- The Executive Headteacher and (at least) another member of the senior leadership team 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.
- The Executive Headteacher will appoint an Online Safety Lead in each school.
- The Executive Headteacher is responsible for ensuring that Designated Safeguarding Leads / Online Safety Lead, IT provider/technical staff, 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.
- The Executive Headteacher 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.
- The Executive Headteacher will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.

- The Executive Headteacher/senior leaders will work with the safeguarding governor, the designated safeguarding lead (DSL) teams and IT service providers in all aspects of filtering and monitoring.

#### 4.3 Governors

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

“Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children’s welfare .... this includes ... online safety”

“Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)”

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 safeguarding governor who 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 Designated Safeguarding Lead / Online Safety Lead
- 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. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards
- Sharing monitoring reports with the local governing body
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards

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

#### 4.4 Designated Safety Lead (DSL)

*Keeping Children Safe in Education states that:*

*“The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder’s job description.”*

*They (the DSL) “are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college”*

*They (the DSL) “can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online”*

The DSL will:

- hold the overall oversight of 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 safeguarding governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings
- 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 IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

#### *4.5 Online Safety Lead*

The Online Safety Lead will:

- work closely on a day-to-day basis with the Designated Safeguarding Lead (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 curriculum leaders 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/carers/pupils
- 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

#### *4.6 Curriculum Leads*

Curriculum Leads for Computing and PSHE/RHSE will work with the DSL/OSL to develop a planned and coordinated online safety education programme

This will be provided through:

- PHSE and RSHE programmes

- A mapped cross-curricular programme
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. *Safer Internet Day* and *Anti-bullying week*.

#### 4.7 Teaching and support staff

All school staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement
- they follow all relevant guidance and legislation including, for example, [Keeping Children Safe in Education](#) and [UK GDPR regulations](#)
- all digital communications with pupils, parents and carers and others should be on a professional level *and only carried out using official school systems and devices (where staff use AI, they should only use trust-approved AI services for work purposes which have been evaluated to comply with organisational security and oversight requirements)*
- they immediately report any suspected misuse or problem to a DSL (if related to a child) or the Executive Headteacher (if related to an adult in school) for investigation/action, in line with the school safeguarding procedures
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure 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, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned 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.
- they have a general understanding of how the pupils in their care use digital technologies out of school, in order to be aware of online safety issues that may develop from the use of those technologies

## 4.8 IT Provider

The DfE Filtering and Monitoring Standards says:

*“Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider.”*

*“Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support.”*

*“The IT service provider should have technical responsibility for:*

- maintaining filtering and monitoring systems*
- providing filtering and monitoring reports*
- completing actions following concerns or checks to systems”*

*“The IT service provider should work with the senior leadership team and DSL to:*

- procure systems*
- identify risk*
- carry out reviews*
- carry out checks”*

*“We are aware that there may not be full-time staff for each of these roles and responsibility may lie as part of a wider role within the school, college, or trust. However, it must be clear who is responsible, and it must be possible to make prompt changes to your provision.”*

The schools have an external IT provider (JC Comtech). However, it remains the responsibility of the school to ensure that the provider carries out all the online safety measures that the school's obligations and responsibilities require. It is also important that the provider follows and implements school Online Safety Policy and procedures.

The IT Provider is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- 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 / MAT 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 DSLs 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*

### *Pupils*

- are responsible for using the school digital technology systems in accordance with the learner 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.
- should recognise the importance of citing where work is taken from another source.

### *4.9 Parents and carers*

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

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 a copy of the pupils' acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images, cloud services etc.
- parents'/carers' 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.*
- *Reinforcing the expectation – outlined in the schools' Mobile Phone Policy' – that no personal devices are to be used by pupils in school*

### *4.10 Community users*

Community users who access school systems/website/learning platform as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems.

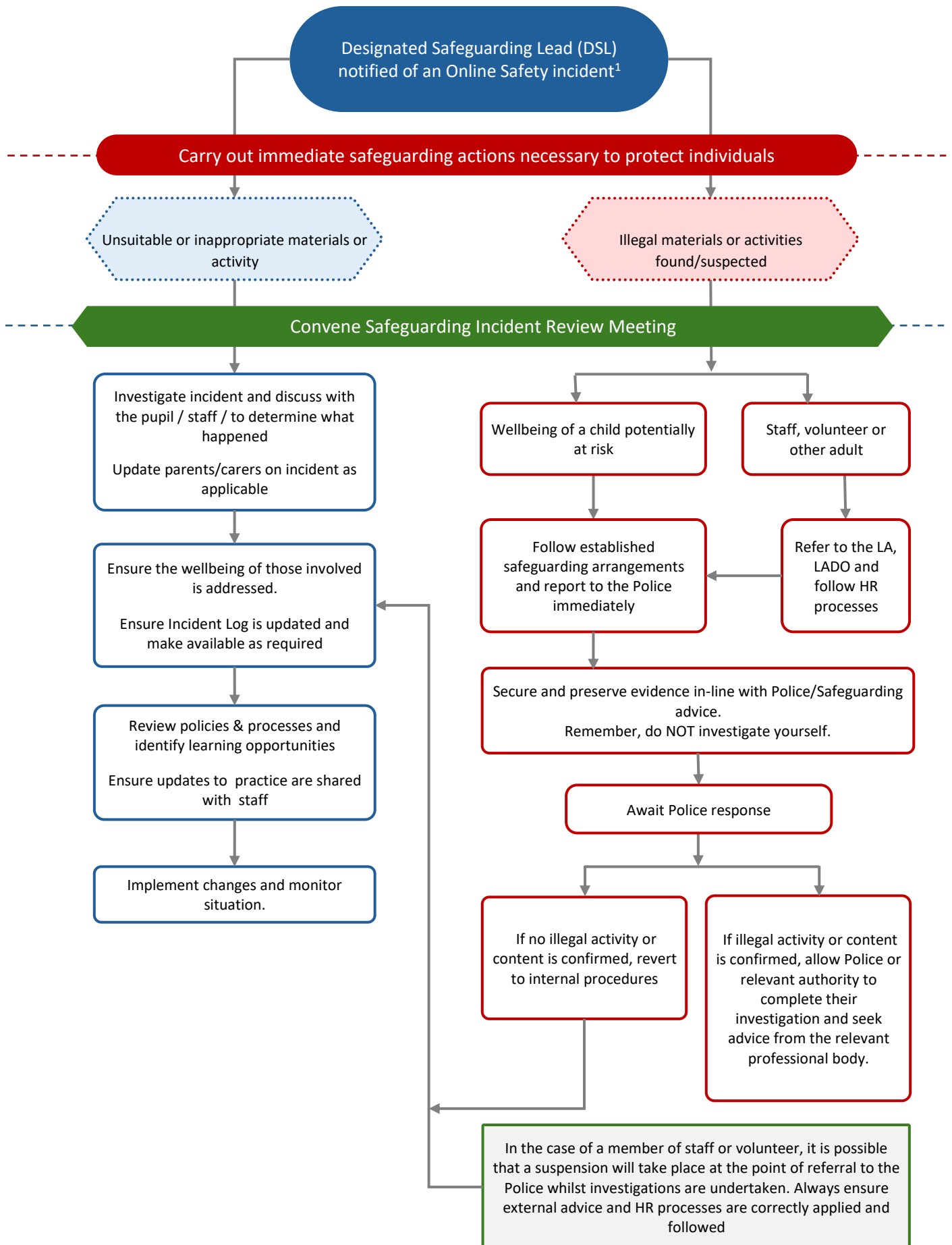
*The school encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other schools and the community.*



## 5.0 Responding to online safety incidents

DSLs will always respond to an online safety incident (as triggered by any notification from the schools' monitoring system, or raised directly by a member of the school community).

The response taken will depend on the nature of the incident.



## 6.0 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 JC Comtech 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, as laid out in the Service Level Agreement.

The filtering and monitoring provision is reviewed at least annually by the Executive Headteacher and Designated Safeguarding Lead, with the involvement of the IT Service Provider.

### 6.1 Filtering

The DfE Technical Standards for Schools and Colleges states:

*“Schools and colleges have a statutory responsibility to keep children and young people safe online as well as offline. Governing bodies and proprietors should make sure their school or college has appropriate filtering and monitoring systems in place, as detailed in the statutory guidance, [Keeping children safe in education](#).*

*Filtering is preventative. It refers to solutions that protect users from accessing illegal, inappropriate and potentially harmful content online. It does this by identifying and blocking specific web links and web content in the form of text, images, audio and video.*

*These standards help school and college leaders, designated safeguarding leads and IT support understand how to work together to make sure they can effectively safeguard their students and staff.”*

The Executive Headteacher and safeguarding governor are responsible for ensuring these standards are met. Roles and responsibilities of staff and third parties, for example, in-house or third-party IT support are clearly defined.

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. These are acted upon in a timely manner, within clearly established procedures
- 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 Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- There are regular checks of the effectiveness of the filtering systems . Checks are undertaken across a range of devices at least termly and the results recorded and analysed to inform and improve provision. The DSL and Governor are involved in the process and aware of the findings.
- Devices that are provided by the school have school-based filtering applied irrespective of their location.
- *the school has (if possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/pupils, etc.)*
- *younger pupils will use child friendly/age-appropriate search engines*
- *the school has a mobile phone policy and where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.*
- *access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.*

If necessary, the school will seek advice from, and report issues to the relevant authority.

## 6.2 Monitoring

[The DfE Technical Standards for Schools and Colleges](#) states:

*“Monitoring is reactive. It refers to solutions that monitor what users are doing on devices and, in some cases, records this activity. Monitoring can be manual, for example, teachers viewing screens as they walk around a classroom. Technical monitoring solutions rely on software applied to a device that views a user’s activity. Reports or alerts are generated based on illegal, inappropriate, or potentially harmful activities, including bullying. Monitoring solutions do not block users from seeing or doing anything.”*

The school follows the UK Safer Internet Centre [Appropriate Monitoring](#) guidance.

The school has monitoring systems in place, agreed by senior leaders and technical staff, 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 monitoring is in place.

- 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 monitoring provision is reviewed at least once every academic year and updated in response to changes in technology and patterns of online safety incidents and behaviours. The review should be conducted by members of the senior leadership team, the designated safeguarding lead, and technical staff. It will also involve the responsible governor. The results of the review will be recorded and reported as relevant.
- Devices that are provided by the school have school-based monitoring applied irrespective of their location.
- monitoring enables alerts to be matched to users and devices.

## 7.0 Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended standards in the [DfE Technical Standards for Schools and Colleges](#)

- responsibility for technical security resides with the Executive Headteacher who may delegate activities to identified roles.
- A documented access control model is in place, clearly defining access rights to school systems and devices. This is reviewed annually. All users (staff and pupils) 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. Users must immediately report any suspicion or evidence that there has been a breach of security
- password policy and procedures are implemented and are consistent with guidance from the National Cyber Security Centre
- all school networks, devices and system will be protected by secure passwords.
- the administrator passwords for school systems are kept in a secure place, e.g. school safe.
- 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 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 Executive Headteacher is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that, through the schools' IT provider, 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, as agreed)

- use of school devices out of school and by family members 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 without the consent of the Executive Headteacher /IT service provider
- removable media is not permitted unless approved by the SLT/IT service provider
- systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- guest users are provided with appropriate access to school systems based on an identified risk profile.
- systems are in place that prevent the unauthorised sharing of personal / sensitive data unless safely encrypted or otherwise secured.
- Care will be taken when using Artificial Intelligence services to avoid the input of sensitive information, such as personal data, internal documents or strategic plans, into third-party AI systems unless explicitly vetted for that purpose. Staff must always recognise and safeguard sensitive data.
- dual-factor authentication is used for sensitive data or access outside of a trusted network
- where AI services are used for technical security, their effectiveness is regularly reviewed, updated and monitored for vulnerabilities.
- Where AI services are used, the school will work with suppliers to understand how these services are trained and will regularly review flagged incidents to ensure equality for all users e.g. avoiding bias

## 8.0 Online Publishing

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

- Public-facing website
- Social media
- Online newsletters

The school website is managed/hosted by ‘The Specialists’ (<https://www.thespecialists.org.uk/>). The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected, and full names are not published.

*The school public online publishing provides information about online safety e.g., publishing the schools Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc, creating an online safety page on the school website.*

*The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process.*

## 9.0 Cyber Security

The DfE Cyber security standards for schools and colleges explains:

“Cyber incidents and attacks have significant operational and financial impacts on schools and colleges. These incidents or attacks will often be an intentional and unauthorised attempt to access, change or damage data and digital technology. They could be made by a person, group, or organisation outside or inside the school or college and can lead to:

- safeguarding issues due to sensitive personal data being compromised
- impact on student outcomes
- a significant data breach
- significant and lasting disruption, including the risk of repeated future cyber incidents and attacks, including school or college closure
- financial loss
- reputational damage”

The trust has overall responsibility for adherence to the DfE Cybersecurity standards for school and colleges and the Executive Headteacher work in conjunction with trust leaders in their implementation.

## 10.0 Related policies

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

- Anti-Bullying Policy
- Safeguarding policy
- Mobile Phone Policy
- RSHE Policy
- GDPR Policy
- Staff Code of Conduct