Kingsmead School

Online Safety

Procedure

Audience: Staff/Governors/Students

Frequency of Review: Annually

Post Holder responsible for Review: Designated Safeguarding Lead

Recommended associated documents:

- Safeguarding Procedure 2026/2027
- Kingsmead Rewards Sanctions Strategy
- JTMAT ICT Security - Password Policy
- JTMAT ICT Security - Backup Policy
- JTMAT ICT Security - Acceptable Use Policy

Date of Last Review	September 2026
Date of Next Review	September 2027

Kingsmead School

School Online Safety

Background / Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. School on-line safety guidance should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Head of School and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this on-line safety guidance is used in conjunction with other school policies (e.g., behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The on-line safety guidance that follows explains how we intend to do this, while also addressing wider educational issues to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Our approach to online safety is based on addressing the 4 key categories of risk:

- Content- being exposed to illegal, inappropriate or harmful content such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-semitism, radicalisation and extremism.
- Contact- being subjected to harmful online interaction with other users, such as child-to-child pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- Conduct- personal online behaviour that increases the likelihood of, or causes harm such as making, sending, receiving and sharing explicit images and cyber bullying.
- Commerce- risks such as online gambling, inappropriate advertising, phishing and/or financial scam.

Schedule for Development / Monitoring / Review

This online safety guidance was approved by the Governing Body/ Governors subcommittee on:	Date:
The implementation of this online safety guidance will be monitored by the:	DSL and Technicians
Monitoring will take place at regular intervals:	Annually
The Governing Body / Sub Committee will receive a report on the implementation of the online safety guidance from the DSL through the Link Governor for On-line safety	Half yearly
The Online Safety Guidance will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to on-line safety or incidents that have taken place.	Updated April 2023 Updated September 2023 Updated September 2024 Updated September 2025 Updated September 2026

The school will monitor the impact of the policy using:

- Logs of reported incidents on 'My Concern'
- Logs of internet activity (including sites visited) through Securus

- logs of internet activity through the filtering/firewall software, Securus
- Internal monitoring data for network activity through Securus
- The DSL will receive a full report twice a week through the Securus software

Scope of the guidance

This guidance applies to all members of the school community (including staff, student's volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Head of Schools, to such extent as is reasonable, to regulate the behaviour of students 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 cyber-bullying or other on-line safety incidents covered by this guidance, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this guidance and associated behaviour and antibullying policies/procedures and will, where known, inform parents / carers of incidents of inappropriate on-line safety behaviour that take place out of school.

Legislation and guidance

This policy is based on the Department of Education's statutory safeguarding guidance, Keeping Children Safe In Education and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying including cyber bullying
- Relationships by sex education
- Searching, screening and confiscation
- Protecting children from radicalisation

It reflects existing legislation, including but not limited to the Education Act 1996 , the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, and Online Safety Act 2023 (with updates in the Online Safety Act 2025) and Keeping Children Safe in Education 2026 which gives school professionals the power to tackle cyber- bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' devices where they believe there is a 'good reason' to do so.

This policy also considers the National curriculum computing programmes of study. Non-statutory guidance from the DfE on sharing nude and semi-nude images is available here and is used to support the response to incidents of misuse section of this procedure.

Roles and Responsibilities

The following section outlines the roles and responsibilities for on-line safety of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the Online Safety Guidance and for reviewing the effectiveness of the guidance. This will be carried out by the Governors receiving regular information about on-line safety incidents and monitoring reports. A member of the Governing Body has taken on the role of On-line safety Governor. The role of the On-line Safety Governor will include regular meetings with the DSL. The governors will be aware of regular monitoring of on-line safety incident logs.

The Headteacher

- The Head of School is responsible for ensuring the safety (including on-line safety) of members of the school community, though the day-to-day responsibility for on-line safety will be delegated to the DSL.
- The Headteacher / DSL are responsible for ensuring that all staff receive suitable CPD to enable them to carry out their on-line safety roles and to train other colleagues, as relevant
- The Headteacher / DSL will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal on-line safety monitoring role. This is to provide a safety net and support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the DSL
- The Head of School and Senior Leaders should be aware of the procedures to be followed in the event of a serious on-line safety allegation being made against a member of staff.
- Communication of the JT MAT policy on the use of AI 2026-JTMAT-AI-Policy.pdf and ensuring staff are aware of the policy and the guidance given to staff across the school

On-line Safety Coordinator / DSL

- Takes day to day responsibility for on-line safety issues and has a leading role in establishing and reviewing the school on-line safety guidance / documents
- **Mandatory staff training:** Explicit scheduling for annual online safety training updates and bi-annual child protection/safeguarding training for Designated Safeguarding Leads (DSLs) and deputies
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- **Filtering and monitoring protocols:** Daily log reviews by designated IT staff, clear pathways for reporting unusual internet traffic to the DSL, and updated web-blocking categories (covering CSAM, extremist content, and online harms through the review of Securus, a JT MAT wide used filtering and monitoring system.
- Provides appropriate education and provision to students through the PSHE programme
- Information sharing with Parents on contextual and relevant issues, including guidance from external bodies

- **AI-generated threats:** Ensure Safeguarding procedures are followed for handling AI-generated risks, such as deepfakes, non-consensual image manipulation, or targeted misinformation
- Liaises with MAT and school ICT technical staff, receives reports of on-line safety incidents and creates a log of incidents to inform future on-line safety developments,
- Meets regularly with On-line safety Governor to discuss current issues, review incident logs and filtering / change control logs
- Attends relevant meeting / committee of Governors
- Supporting the Head of School in ensuring that staff and volunteers understand this guidance and that it is being implemented consistently through the school.
- Working with the Headteacher, ICT technical team and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring that online safety incidents are logged through 'My Concern' and dealt with appropriately in line with the school's Behaviour – Rewards and Sanctions Strategy
- Ensuring that any incidents of cyber-bullying are logged through 'My Concern' and dealt with appropriately in line with the school's Behaviour – Rewards and Sanctions Strategy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Head of School and/or local advisory bodies

- Clear implementation and monitoring of mobile phone restrictions or prohibitions during the school day in line with DfE expectations Mobile phones in schools - GOV.UK

Strategic Network Manager and IT support are responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- That users may only access the school's networks through a properly enforced password protection policy,

- The school's filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- That he / she keeps up to date with on-line safety technical information in order to effectively carry out their on-line safety role and to inform and update others as relevant
- That the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the DSL /Head of School / Senior Leader / Head of ICT / Class teacher / Progress Leader (as in the section above) for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in school policies and guidance
- Blocking access to potentially dangerous sites and, where possible, preventing the download of potentially dangerous files

Teaching and support staff (All staff and volunteers) are responsible for ensuring that:

- They have an up-to-date awareness of on-line safety matters and of the current school On-line Safety guidance and practices
- They have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- They report any suspected misuse or problem to the DSL /Head of School / Senior Leader / Head of ICT / ICT Co-ordinator / Class teacher / Progress Leader (as in the section above) for investigation / action / sanction, through 'My Concern'
- Digital communications with students should be on a professional level and only carried out using official school systems
- Students understand and follow the school on-line safety and acceptable use policy
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra-curricular and extended school activities
- They are aware of on-line safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school policies and guidance regarding these devices.
- In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use Any unsuitable material found by a student should be reported immediately via 'My concern' to the DSL.

Students

- Are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to school systems
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- Are responsible and expected to adhere to the school's Mobile Phone Guidance Mobile-Phone-Guidance-2026.pdf
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.

  Should understand the importance of adopting good on-line safety practice when using digital technologies out of school and realise that the school's On-line Safety Guidance covers their actions out of school, if related to their membership of 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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, and website. Parents and carers will be responsible for:

- Endorsing (by signature) the Student Acceptable Use Policy
- Should notify a member of staff or the Head of School of any concerns of queries regarding this guidance.
- Ensure their child has read/understood and agreed to the acceptable use forms and conditions.

Community Users

Community users who access school ICT systems / website as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

Policy Statements this Guidance should be cross referenced with the following policies

- Kingsmead Rewards Sanctions Strategy
- JTMAT ICT Security Policy – Backup Policy
- JTMAT ICT Security - Password Policy
- JTMAT ICT Security - Acceptable Use Policy

Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in on-line safety is therefore an essential part of the school's on-line safety provision. Children and young people need

the help and support of the school to recognise and avoid on-line safety risks and build their resilience. On-line Safety education will be provided in the following ways:

- A planned on-line safety programme should be provided as part of ICT, Assembly and Tutor programs and drop-down days, and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school

  Key On-line safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students 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
- Students should be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet will be posted in all rooms and displayed on log-on screens
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – parents / carers

Many parents and carers have only a limited understanding of on-line 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 on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report). The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, website
- Parents evenings
- Parent partnership evenings

Technical – infrastructure / equipment, filtering and monitoring

The school will be 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 will also need to ensure that the relevant people named in the above sections will be effective in carrying out their on-line safety responsibilities.

- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users are be recorded by the ICT technical team
- All users will be provided with a username and password by the school who will use automated software provided by the trust to maintain and manage accounts.

- Users will be made responsible for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school implements a system of filtering and monitoring through Entrust. All online activity on school computers is monitored by a company called Securus and staff receive notification if there are any concerning searches or content.
- Our filtering system ensures that no inappropriate content can be searched. IT along with the DSL decide if a site can be unblocked for educational purposes and this is logged and reviewed.

- Any filtering issues should be reported immediately to the ICT technical team and DSL.
- Requests from staff for sites to be removed from the filtered list will be considered by the senior ICT professional onsite along with the DSL.
- School regularly monitor and record the activity of users via Securus or other acceptable system on the school ICT systems and users are made aware of this in the Acceptable Use Policy
- Remote management tools are used by staff to control workstations and view users' activity
- An appropriate system is in place for users to report any actual / potential on-line safety incident to the ICT technical team (or other relevant person).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- Agreed procedures are in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices
- The school infrastructure and individual workstations are protected by up-to-date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

On-line safety should be a focus in all areas of the curriculum and staff should reinforce on-line safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, e.g. using search engines, 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, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need through the DSL.
- Specific sessions on Online Safety provided through Personal Development in the PSHE Programme
- Students 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
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Training

All staff to receive training on safe internet use and online safeguarding issues upon induction (leadership journal). The key level 1 training highlights risks of online safety. Annual refresher on safeguarding training including new updates. This training will inform staff:

- Technology is a large component in safeguarding issues
- Abuse can be done online through messages of an abusive, misogynistic and harassing nature. Non-consensual sharing of indecent images and/or videos. Sharing of abusive images and pornography to those who do not want to receive this content.
- Physical abuse, sexual violence and intimidation type violence can all contain an online element.

Will assist in raising staff awareness to help spot the signs and symptoms of online abuse. It will help staff influence students to use online platforms in a safe and healthy way. DSL and deputies to take child protection and safeguarding training (which include online safety) every 2 years. This will update their knowledge on online safety. Governors to receive contextual updates at regular meetings. Volunteers to Kingsmead will receive appropriate updates and training.

Official Use of Social Media:

Staff official use of social media

- If staff are participating in online activity as part of their capacity as an employee of John Taylor MAT, then they are requested to be professional at all times and that they are an ambassador for the trust and their home school, Kingsmead.
- Staff using social media official will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Staff using social medial officially will always act within the legal frameworks they would adhere to within Kingsmead including: libel; defamation, confidentiality; copyright; data protection as well as equalities laws.

Staff must ensure that any image posted on Kingsmead school's social media channels have appropriate written parental consent.

- Staff using social medial officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of Kingsmead unless they are authorised to do so.
- Staff will not engage with any direct or private messaging with students or parents/carers through social media and should communicate via Kingsmead communication channels.
- Staff using social media officially will sign a Kingsmead AUP before official social media use will take place

Staff personal use of Social Media

- Personal use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction (safeguarding training) and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all staff (including volunteers).

- All staff are advised not to communicate with or add as 'friends' any current or past students or current or past students' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with the DSL.
- If ongoing contact with students is required once they have left Kingsmead School's roll, then members of staff will be expected to use existing alumni networks or use official Kingsmead provided communication tools.
- Staff must not use personal accounts or information to contact students or parents, nor should any contact be accepted, except in circumstances whereby prior approval has been given by the Head of School.
- Any communication from students/parents received on personal social media accounts will be reported to the DSL.
- Information that staff have access to as part of their employment, including photos and personal information about students and their family members, colleagues etc. will not be shared or discussed on personal social mediate sites.
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listing on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and should ensure that their social media use is compatible with their professional role.
- Members of staff will be encouraged to manage and control the contents they share and post online.
- Members of staff are advised not to use private messenger services (such as WhatsApp or Facebook messenger) to discuss school matters and/or student's/staff members unless officially sanctioned by the school.

Students use of social media

- Safe and responsible use of social media sites will be outlined for students and their parents.
- Students will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and/or their location. Examples would include real /full name, address, mobile or landline phone numbers, school attended, instant messenger contact details, information through photographs, email addresses, full names of friends/family, specific interests and clubs etc.
- Students will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- Students will be advised on appropriate security on social media sites and will be encouraged to use safe passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Students will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.

Any concerns regarding students' use of social networking, social media and personal publishing sites, both at home and at Kingsmead will be dealt with in accordance with existing Kingsmead

policies/guidance including anti-bullying and behaviour. Concerns will be raised with their parents/carers, particularly when concerning any underage use of social media sites.

Staff use of personal devices and mobile phones

- Members of staff are not permitted to use their own personal phones or devices for contacting students, young people and their families within or outside of Kingsmead in a professional capacity. Any pre-existing relationships which could compromise this must be discussed with the DSL.
- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of students and will only use work-provided equipment for this purpose.
- Staff will not use any personal devices directly with students and will only use work-provided equipment during lessons/educational activities.
- Staff personal mobile phones should not be visible in the classroom areas and/or corridors. Staff should only use their personal mobile phones in office areas during non-contact time.
- If a member of staff is thought to have illegal contents saved or stored on a mobile phone or personal device or have committed a criminal offence, then the police will be contacted, and allegations will be responded to.

Visitors use of personal devices and mobile phones

- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos is not permitted unless permission is granted by the DSL.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the DSL of any breaches of use by visitors.

School devices off site

All students who have a loaned laptop for one day will not need to sign an agreement. However, long term loaning of laptops will require parents to sign an agreement form. Students/ families are liable for costs associated with damaged to these loaned items. Before being given the laptops, students are made aware they are monitored using software. The students are informed via the acceptable use form that inappropriate use will be followed up by pastoral/ safeguarding teams. Laptops must only be used for educational purposes or for members of the household who do not have authorised access to Kingsmead network. The student's user and password should not be shared with anyone else.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

There are many reported incidents of employers carrying 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 students 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.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

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**.** Staff and students 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 need to be aware that email communications may be monitored
- Users must immediately report, to the DSL/Head of School, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students / pupils or parents / carers (email, chat,) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Students will be provided with individual school email addresses for educational use
- Students should be taught about email safety issues, such as the risks attached to the use of

- personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website, and only official email addresses should be used to identify members of staff.

Responding to incidents of misuse

It is expected that all members of the school community will be responsible users of ICT, who understand and follow these procedures and guidance. However, there may be times when infringements could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

If any misuse is apparent, for student concerns should be reported through 'My Concern'. For the staff misuse all incidents should be reported to the Head of School or DSL immediately.

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.

Filtering and monitoring

Roles and responsibilities

All staff

All staff are responsible for ensuring they are safe online and comply with the JTMAT Acceptable User Policy. All staff are responsible for reporting any concerns about online safety. Student online safety concerns are reported via MyConcern. Staff online safety concerns are reported on confide (DSL and Headteacher). Concerns about filters, including allowing access and blocking access must be discussed with the DSL. Teaching staff using computer facilities around school are responsible for ensuring students are using the IT equipment and online facilities in a safe way. Teaching staff in IT rooms are responsible for physically monitoring the use of IT facilities as well as ensuring the remote monitoring of the IT facilities using LAN Schools software. Teaching staff who need support using the remote monitoring software must speak to the IT Support Team to access training on this prior to using the computer rooms.

Governors

The Governing Body is responsible for ensuring that the school meets the requirements of KCSIE, 2024 and the published safety standards.

DSL/ deputies

The DSL has the lead responsibility for Online safety, filtering and monitoring. The DDSL will support the day-to-day management of online safety referrals.

Headteacher/DSL

Both have responsibility for checking and monitoring Securus (school online monitoring system) and responding to concerns raised by Securus

SLT/ Headteacher

Pastoral Staff including progress leaders may be involved in supporting and investigating concerns related to online safety, including issuing sanctions in line with the Behavior Management Procedure where appropriate. The SLT are responsible for ensuring that IT provision in school is adequately meeting the needs of staff and students, balancing the need for effective safeguarding, filtering and monitoring with providing high quality teaching and learning.

IT support staff

Are responsible for the day-to-day maintenance of the IT infrastructure and filtering in place on the school network. Are responsible for running the filtering checks and sharing the reports with the DSL. Are responsible for running a termly report on updated (added/removed) filters with reasons and sharing this with the DSL. Are responsible for keeping a record of all tickets logged via the helpdesk related to filtering.

Filtering

The school has multiple layers of filtering based on each user group. The filters apply to all devices that use the school network. The strategic ICT lead for JTMAT can see all Kingsmead filtering categories. Some filtering at the source is padlocked meaning there no control for Kingsmead to adapt or edit the level of filtering. Kingsmead school can select additional filters on top of those added at the source by contacting and liaising with the IT support staff. Consultation with the DSL is required should staff require filters being removed to allow access to specific material. Below are the multiple layers of filtering, subcategories may be added when required:

Group 1- students (most restricted)

Group 2- staff

Group 3- specialist users (least restrictive).

Monitoring

Kingsmead school IT systems are monitored using Securus. All captures are reviewed and assigned a grading from 1 to 5, with 5 being the most significant. Securus monitor captures and inform the DSL and headteacher if there are any concerning searches. Concerning captures are followed up with and added to Myconcern. Emerging patterns or trends relating to online safety is shared with PSHE lead to provide preventative education to the curriculum. The behaviour lead and progress leaders may be involved in supporting the investigation of online safety incidents and sanctioning in line with the JTMAT behaviour policy and Kingsmead behaviour procedure.

All staff have responsibility to monitor and inform of any harmful material or unfiltered websites to the DSL to ensure access to these materials/ websites are removed. This procedure will be reviewed annually by the DSL. At every review, the procedure will be shared with the governing board and staff.