Online Safety Policy

Policy Type:	IT and Safeguarding
Updated:	September 2024
Next Review:	September 2025

Online Safety Policy

1. Statement of intent

At the James Montgomery Academy Trust (JMAT) we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for children and play an important role in their everyday lives.

JMAT and its schools recognises that today's children are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks. The JMAT Online Safety policy and day-to-day online safety procedures have due to regard to the most recent DFE non-statutory guidance entitled 'Teaching online safety in school' (June 2019). This helps teach our children how to stay safe online, within both new and existing school subjects (including Relationships Education, Relationships and Sex Education, Health Education, Citizenship and Computing). We teach children about the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app.

JMAT is committed to providing a safe learning and teaching environment for all children and staff, and has implemented important controls to prevent any harmful risks.

JMAT has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all children and staff.

2. Legal framework

This policy has due regard to statutory legislation, including, but not limited to, the following:

- The Human Rights Act 1998
- The Data Protection Act 2018 (GDPR)
- The Regulation of Investigatory Powers Act 2000
- The Safeguarding Vulnerable Groups Act 2006
- The Education and Inspections Act 2006
- The Computer Misuse Act 1990, amended by the Police and Justice Act 2006

This policy also has regard to the following DfE guidance:

- DfE (2024) Keeping children safe in education
- DfE (2023) Working together to Safeguard Children
- DfE (2024) Sharing nudes and semi-nudes
- DfE EYFS Framework (2023)
- DfE (2023) The Prevent Duty

3. Use of the internet

The JMAT understands that using the internet is important when raising educational standards, promoting achievement and enhancing teaching and learning.

Wherever possible, staff should use school devices, this ensures that the setting's filtering and monitoring software is enabled. Internet use is embedded in the statutory curriculum and is therefore an entitlement to all children, though there are a number of controls the JMAT is required to implement to minimise harmful risks.

When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including:

- Access to illegal, harmful or inappropriate images.
- Cyber bullying/online abuse.
- Access to, or loss of, personal information.
- Access to unsuitable online videos or games.
- Inappropriate communication with others.
- Illegal downloading of files

- Exposure to explicit or harmful content, e.g. involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge
- Youth Produced Sexual Imagery (YPSI) or 'sexting'

4. Portable equipment

JMAT provides portable ICT equipment such as laptop computers, iPads and other technologies to enhance the children's education and to allow staff to make efficient use of such equipment to enhance their own professional activities.

No portable equipment or devices will be used to bully, harm, intimidate or embarrass another person.

Equipment such as laptop computers are encouraged to be taken offsite for use by staff in accordance with the Staff Code of Conduct.

Staff are required to sign a disclaimer accepting full responsibility for the equipment in their care, and that the equipment is fully insured from the moment it leaves school premises.

No files should be transported off the school site on a memory stick, laptop or similar that contain any personal information about a child or staff including a child or staff's full name. All files leaving the school site should be encrypted and should only be accessible using a 'strong' password.

5. Online meetings/training

When conducting remote meetings with staff and/or parents, all online safety measures must be observed, including those involving data protection and GDPR.

The JMAT Staff Code of Conduct must be followed at all times in relation to appropriate dress and behaviour online, particularly when participating in meetings with outside agencies and those conducted in a professional capacity or when representing school.

This guidance also covers participating in remote training sessions. Staff should be aware that their behaviour online is reflective of school and should be above reproach at all times.

6. Roles and responsibilities

6.1 It is the responsibility of all staff to be alert to possible harm to children or staff, due to inappropriate internet access or use, both inside and outside of schools in the JMAT, and to deal with incidents of such as a priority. This includes the responsible and safe use of mobile phones, cameras and other electronic devices with imaging and sharing capabilities.

6.2 The JMAT Board of Trustees will ensure there is a system in place which monitors and supports the person responsible for online safety, and whose role is to carry out the monitoring of online safety in JMAT schools, keeping in mind data protection requirements.

6.3 The headteacher is responsible for:

- Ensuring that online safety issues are embedded in the curriculum.
- Tat safe internet access is promoted at all times.
- Communicating with parents regularly and updating them on current online safety issues and control measures.
- Providing relevant training and advice for members of staff on online safety as part of the requirement for staff to be able to teach children about online safety.

6.4 The Designated Safeguarding Lead is responsible for:

- Filtering and monitoring (lead responsibility).
- Ensuring the day-to-day online safety in JMAT schools
- Managing any issues that may arise
- Establishing a procedure for reporting incidents and inappropriate internet use, either by childen or staff.

6.5 All JMAT staff are responsible for ensuring they are up-to-date with current online safety issues, and this Online Safety Policy.

Staff should always maintain appropriate professional boundaries, avoid behaviour which could be misinterpreted by others and report any such incident to a senior manager. This is as relevant in the online world as it is in the classroom; staff engaging with children and/or parents online have a responsibility to model safe practice at all times.

6.6 Parents of children in JMAT are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately.

7. Online safety control measures

7.1 Educating children:

- Children will be taught about the importance of online safety and are encouraged to be critically aware of the content they access online, including extremist material.
- Children will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism.
- Clear guidance on the rules of internet use will be presented in all classrooms.
- Children are instructed to report any suspicious use of the internet and digital devices.

7.2 Educating staff:

- All staff will undergo online safety training to ensure they are aware of current online safety issues and any changes to the provision of online safety, as well as updated with current developments in social media and the internet as a whole.
- All staff will be educated on which sites are deemed appropriate and inappropriate.
- All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.
- Teaching staff are responsible for checking the content of online learning prior to using it either in the classroom or remotely

7.3 Internet access:

- Effective filtering systems will be established to eradicate any potential risks to children's inappropriate material.
- The person responsible for online safety in school will ensure that use of appropriate filters and monitoring systems does not lead to "over blocking", such that there are unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding
- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the headteacher
- All JMAT school systems will be protected by up-to-date virus software
- An agreed procedure will be in place for the provision of temporary users, e.g. volunteers and supply staff.

7.4 Email:

- Staff will be given approved email accounts and are only able to use these accounts.
- Use of personal email to send and receive personal data or information is prohibited.
- No sensitive personal data shall be sent to any chldren, staff or third parties via email.
- Any emails sent by children to external organisations will be overseen by their class teacher and must be authorised before sending.
- Chain letters, spam and all other emails from unknown sources will be deleted without opening.

7.5 Social networking:

- Access to social networking sites will be filtered as outlined in the Social Media Policy.

- Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the Headteacher.
- Children are regularly educated on the implications of posting personal data online, outside of the school.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.
- Staff are not permitted to communicate with children over social networking sites and are reminded to alter their privacy settings.
- Staff are not permitted to publish comments about the school which may affect its reputation.

7.6 Published content on the JMAT/school websites and images:

- The CEO/Headteacher will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate.
- Contact details on the website will include the phone number, email and address of the JMAT or school. No personal details (other than name and position, and with consent) of staff or children will be published.
- Images and full names of children, or any content that may easily identify a child, will be selected carefully, and will not be posted until authorisation from parents has been received.
- Staff must not take photographs/videos using their personal equipment (personal phones/tablets/iPads), only school devices must be used for this purpose.
- Any member of staff that is representing the JMAT/school online, e.g. through blogging, remote meetings or training, must be careful to express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputation.

7.7 Mobile devices and hand-held computers:

- Mobile devices are not permitted to be used during school hours by children, this includes mobile phones, cameras and other electronic devices with imaging and sharing capabilities, such as smartwatches such as Gator, Fitbit, Apple Watch, etc – those devices designed to monitor children's movements, particularly those devices able to make or receive phone calls/texts
- During contact time staff mobile phones should be switched to silent and out of sight. Phones can only be on your person and used during non-contact time. Any exceptions to this must be discussed and agreed with headteacher.
- Smartwatches, such as Applewatch, can be worn by staff members but the text function should be turned off during contact time.
- Staff are permitted to use hand-held computers which have been provided by the JMAT, though internet access will be monitored for any inappropriate use by the person in school responsible for online safety when using these on JMAT premises.
- The sending of inappropriate messages or images from mobile devices is prohibited.

8. Reviewing online safety

As technology constantly evolves, along with the risks and harms related to it, the JMAT will carry out an annual review of online safety with JMAT IT Lead and Trust DSL. This will link to appropriate risk assessments, where necessary, to reflect the risks that children face. The headteacher and computing lead in each school in the trust will work in conjunction with the JMAT IT team to ensure that the filtering of websites and monitoring of devices is up-to-date and in place to prevent children accessing any unsuitable or inappropriate material, including that relating to terrorism and extremism.

9. Virus management

Technical security features, such as virus software, are kept up-to-date and managed by the JMAT IT Team.

10. Cyber bullying/online abuse

For the purpose of this policy, "cyber bullying/online abuse" is a form of bullying whereby an individual is the victim of harmful or offensive posting of information, or images, online. The JMAT recognises that both staff and children may experience cyberbullying/online abuse and will regularly educate staff, children and parents on the importance of staying safe online, as well as being considerate to what they post online.

The schools in the JMAT will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and children.

The JMAT has zero tolerance for cyber bullying and/or online abuse, and any incidents will be treated with the utmost seriousness and will be dealt with in accordance with our Anti-Bullying Policy and Child on Child Abuse Policy.

11. Sharing nudes and semi-nudes (youth produced sexual imagery or sexting)

Sharing nudes and semi nudes is defined as the sending or posting of nude or semi-nude images, videos or live streams online by young people under the age of 18. Nudes and semi-nudes can be shared online via social media, gaming platforms, chat apps, forums, or involve sharing between devices using offline services.

The motivations for taking and sharing nude and semi-nudes are not always sexually or criminally motivated. Such incidents are categorised as aggravated or experimental, depending on the context of the incident. Incidents of upskirting and downblousing are included in this section.

Whilst children and young people creating and sharing images can be risky, it is often the result of their natural curiosity about sex and their exploration of relationships. Therefore, engaging in the taking or sharing of nudes and semi-nudes may not always be ‘harmful’ to all children and young people.

Incidents will be considered on a case-by-case context, considering what is known about the children involved and if there is an immediate risk of harm. Often, children and young people need education and support for example, on identifying healthy and unhealthy behaviours within relationships and understanding consent and how to give it. Safeguarding action will also be required in cases where there is risk of harm.

11.1 Procedure to follow in the event of a ‘sharing nudes or semi-nudes’ incident

- Report it to your Designated Safeguarding Lead (DSL) immediately.
- Do not delete the imagery or ask the child to delete it.
- Do not ask the child/children who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL
- Do not share information about the incident with other members of staff, the young person it involves or their, or other, parents and/or carers.
- Do not say or do anything to blame or shame any young people involved.
- Do explain to them that you need to report it and reassure them that they will receive support and help from the DSL
- Parents should be informed and involved at an early stage, in line with advice from police, social care, etc

11.2 The DSL will:

- Hold a meeting with appropriate staff to assess the incident as either aggravated or experimental.
- Interview the children concerned.
- Inform parents/carers at an early stage so they can be involved in the process in order to best support the child or young person (unless there is good reason to believe that involving them would put the child or young person at risk of harm).
- Make a referral to children’s social care and/or the police immediately if there are abusive or aggravating factors to the incident, or if there is a concern that a child or young person has been harmed or is at risk of immediate harm.

11.3 Supporting the child

A child or young person who discloses they are the subject of an incident of sharing nudes and semi-nudes is likely to be embarrassed and worried about the consequences. The member of staff should ensure the child is feeling comfortable and appropriate and sensitive questions are asked, in order to minimise further distress or trauma to them. It is likely that disclosure at school is a last resort, and they may have already tried to resolve the issue themselves. They will need pastoral support both during the disclosure and after the event. It is important that the child is given a sense of control over the reporting process and is supported by a member of staff with whom they have a trustful relationship.

Further detailed guidance for assessing and dealing with an incident of sharing nudes or semi nudes in

school can be found at:

https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people

11.4 Searching devices, viewing and deleting nudes and semi-nudes

Wherever possible, responses to incidents should be based on what the DSL has been told about the content of the imagery. Staff must not intentionally view any nudes and semi-nudes unless the DSL is satisfied there is good reason to do so and that viewing the image:

- Is the only way to make a decision about whether to involve other agencies because it is not possible to establish the facts from the children involved.
- Is necessary to report it to a website, app or suitable reporting agency (such as the IWF) to have it taken down, or to support the child and parent/carer in making a report.
- Is unavoidable because a child has presented it directly to a staff member or nudes or semi-nudes have been found on the school device or network.

The decision to view any imagery should be based on the professional judgement of the DSL and should always comply with JMAT safeguarding and child protection policy and procedures. Imagery should never be viewed if the act of viewing will cause significant distress or harm to any child or young person involved.

11.5 If it is necessary to view the imagery then the DSL should:

- Never copy, print, share, store or save them; this is illegal. If this has already happened, please contact the police for advice and to explain the circumstances.
- Discuss the decision with the headteacher.
- Make sure viewing is undertaken by the DSL/Headteacher and/or another member of the safeguarding or leadership team - this staff member does not need to view the images.
- Wherever possible, make sure viewing takes place on school premises, ideally in the headteacher's office.
- Make sure wherever possible that they are viewed by a staff member of the same sex as the child or young person in the images.
- Record how and why the decision was made to view the imagery on RecordMy, including who was present, why the nudes or semi-nudes were viewed and any subsequent actions.

If any devices need to be taken and passed onto the police, the device should be confiscated and the police should be called. The device should be placed in a secure place, for example in a locked cupboard or safe until the police are able to come and collect it.

See **Appendix 1** for further information on sharing nudes and upskirting.

12. Reporting misuse

12.1 Misuse by children:

- Teachers have the power to discipline children who engage in misbehaviour with regards to internet use.
- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the Designated Safeguarding Lead.
- Any child who does not adhere to the rules and is found to be wilfully misusing the internet, will have a letter sent to their parents explaining the reason for suspending their internet use.
- Complaints of a child protection nature, such as when a child is found to be accessing extremist material, shall be dealt with in accordance with our Safeguarding and Child Protection Policy.

12.2 Misuse by staff:

- Any misuse of the internet by a member of staff should be immediately reported to the headteacher.
- The headteacher will deal with such incidents in accordance with the Allegations of Abuse Against Staff Policy, and may decide to take disciplinary action against the member of staff.
- The headteacher will decide whether it is appropriate to notify the police of the action taken against a member of staff.

13. Handling online safety complaints

Complaints of internet misuse will be dealt with initially by the Headteacher. Any complaint about staff misuse must also be referred to the JMAT CEO/DSL.

Complaints of a child protection nature must be dealt with in accordance with JMAT safeguarding and child protection procedures. Children and parents will be informed of the complaint's procedure.

14. Monitoring and review

This policy will be reviewed annually by the Trust DSL/Trust IT Lead, any changes made to this policy will be communicated to all members of staff. The review will consider the following:

- New legislation and government guidance, including specific guidance issued during specific circumstances.
- Previously reported incidents to improve procedures.
- Latest developments in ICT.
- Feedback from staff/children.

Appendix 1

JMAT - The Legal Position

It is important to be aware that young people involved in sharing sexual videos and pictures may be committing a criminal offence.

Specifically, crimes involving indecent photographs (including pseudo images) of a person under 18 years of age fall under Section 1 of the Protection of Children Act 1978 and Section 160 Criminal Justice Act 1988. Under this legislation it is a crime to:

- Take an indecent photograph or allow an indecent photograph to be taken;
- Make an indecent photograph (this includes downloading or opening an image that has been sent via email);
- Distribute or show such an image;
- Possess with the intention of distributing images;
- Advertise; and
- Possess such images

While any decision to charge individuals for such offences is a matter for the Crown Prosecution Service, it is unlikely to be considered in the public interest to prosecute children. However, children need to be aware that they may be breaking the law. Although unlikely to be prosecuted, children and young people who send or possess images may be visited by police and on some occasions media equipment could be removed. This is more likely if they have distributed images. The decision to criminalise children and young people for sending these kinds of images is a little unclear and may depend on local strategies.

However, the current Association of Chief Police Officers (ACPO) position is that:

'ACPO does not support the prosecution or criminalisation of children for taking indecent images of themselves and sharing them. Being prosecuted through the criminal justice system is likely to be upsetting and distressing for children especially if they are convicted and punished. The label of sex offender that would be applied to a child or young person convicted of such offences is regrettable, unjust and clearly detrimental to their future health and wellbeing.'

However, there are cases in which children and young people have been convicted and sent to prison. The important thing to remember is that whilst, as a school, we will want to consider the implications of reporting an incident over to the police, it is not our responsibility to make decisions about the seriousness of the matter; that responsibility lies with the Police and the CPS hence the requirement for the school to refer.

In summary YPSI/ sexting is classed as illegal as it constitutes sharing and/or possessing an indecent image of a child.

Voyeurism Offences Act 2019

The Voyeurism (Offences) Act 2019 creates 2 new offences criminalising someone who operates equipment or records an image under another person's clothing (without that person's consent or a reasonable belief in their consent) with the intention of viewing, or enabling another person to view, their genitals or buttocks (with or without underwear), where the purpose is to obtain sexual gratification or to cause humiliation, distress or alarm.

The offences will be will carry a maximum 2 year prison sentence.