ONLINE SAFETY POLICY

September 2023

Date for Review: September 2024

JAMES MONTGOMERY
Academy Trust

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 pupils and play an important role in their everyday lives.

The JMAT and its schools recognises that today's pupils 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 pupils 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 pupils 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.

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

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

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 statutory guidance:

- DfE (2023) 'Keeping children safe in education'
- Working together to Safeguard Children 2018 (updated 2020)
- Prevent Guidance for schools 2015

This policy also has regard to the following non-statutory guidance:

- Safer Working Practices (April 2020) – Safer Recruitment Consortium

Use of the internet

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

Wherever possible, staff should use school devices, and contact pupils only via the pupil school email address/log in. 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 pupils, 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'

Portable Equipment

- The JMAT provides portable ICT equipment such as laptop computers, word processors and digital cameras 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 pupil or staff including a pupil or staff's full name. All files leaving the school site should be encrypted and should only be accessible using a 'strong' password.

Conducting Remote Meetings

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

The 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.

Roles and responsibilities

It is the responsibility of all staff to be alert to possible harm to pupils 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.

The **Governing Body** of each school in the trust is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard pupils.

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.

The **Headteacher** is responsible for:

- ensuring that online safety issues are embedded in the curriculum
- that 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 pupils about online safety.

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 pupils or staff.

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 pupils and/or parents online have a responsibility to model safe practice at all times.

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

Online safety control measures

Educating pupils:

- Pupils 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.
- Pupils 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.
- Pupils are instructed to report any suspicious use of the internet and digital devices.

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

Internet access:

- Effective filtering systems will be established to eradicate any potential risks to pupil'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 pupils 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.

- Staff are able to use the internet for personal use during out-of-school hours, as well as break and lunch times.

Inappropriate internet access by staff may result in the staff member being permitted to use the internet for school purposes only, and no personal devices. This will be dealt with following the process outlined in this policy.

Email:

- Pupils and 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 other pupils, staff or third parties via email.
- Any emails sent by pupils 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.

Social networking:

- Access to social networking sites will be filtered as appropriate.
- 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.**
- Pupils 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 pupils 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.
- Staff are not permitted to access social media sites during teaching hours unless it is justified to be beneficial to the material being taught. This will be discussed with the **Headteacher** prior to accessing the social media site.

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 pupils will be published.
- Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully, and will not be posted until authorisation from parents has been received.
- Staff are able to take photographs, though they must do so in accordance with school policies in terms of the sharing and distribution of such. 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.

Mobile devices and hand-held computers:

- Mobile devices are not permitted to be used during school hours by pupils, this includes 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 be locked away in a secure location (classroom cupboard, etc).** 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 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.

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. This will link to appropriate risk assessments, where necessary, to reflect the risks that children face.

The JMAT will ensure that suitable filtering and monitoring systems are in place to prevent children accessing any unsuitable or inappropriate material, including that relating to terrorism and extremism.

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

The person responsible for Online Safety in each school in the trust will work in conjunction with the JMAT IT team to ensure that the filtering of websites and downloads is up-to-date and monitored.

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 pupils may experience cyberbullying/online abuse and will regularly educate staff, pupils 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 pupils.

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.**

'Sexting' or 'sharing nudes' is one of a number of 'risk-taking' behaviours associated with the use of digital devices, social media or the internet. It is accepted that young people experiment and challenge boundaries and therefore the risks associated with 'online' activity can never be completely eliminated.

The JMAT recognises its duty of care to its young people who do find themselves involved in such activity as well as its responsibility to report such behaviours where legal or safeguarding boundaries are crossed.

The definition of Youth Produced Sexual Images/sharing nudes for the purposes of this policy is 'Images or videos generated':

- by children under the age of 18
- or of children under the age of 18 that are of a sexual nature or are indecent.'

These images are shared between children, young people and/or adults via a mobile phone, handheld devices, computer, 'tablet' or website with people they may not even know.

How a safeguarding concern such as sharing an indecent image will be dealt with on a case to case basis,

in consultation with the children concerned, parents and other agencies as appropriate, for example police or social care.

Procedure to follow in the event of a 'sharing nudes' incident
A student is likely to be very distressed especially if the image has been circulated widely and if they don't know who has shared it, seen it or where it has ended up. They will need pastoral support during the disclosure and after the event. They may even need immediate protection or a referral to police or social services; **parents should be informed as soon as possible (police advice permitting).**

'Sharing nudes' disclosures should follow the normal safeguarding practices and protocols (see Safeguarding and Child Protection Policy).

Upskirting/Down-blousing
As of April 2019 'upskirting' is classified as an offence under the Voyeurism Act – offenders are subject to up to 2 years in prison and can be placed on the sex offenders register. Upskirting typically involves taking a photo under a person's clothing without them knowing, with the intention of posing the image online. Similarly down-blousing has the same intention.

Searching a mobile device
The policy allows for a device to be examined, confiscated and securely stored if there is reason to believe it contains indecent images or extreme pornography.

When searching a mobile device, the following conditions should apply:

- The search is conducted by the **Headteacher** or a person authorised by them and one other person
- A member of the safeguarding team should normally be present
- The search should normally be conducted by a member of the same gender as the person being searched. However, if the image being searched for is likely to be of a different gender to the person 'in possession' then the device should only be viewed by a member of the same gender as the person whose image it is.

If any illegal images of a young person are found the DSL/Headteacher will discuss this with the police.

Always put the young person first. Do not search the device if this will cause additional stress to the student/person whose image has been distributed. Instead rely on the description by the young person, secure the advice and contact the Police.

Supporting a pupil
There may be many reasons why a student has engaged in YPSI/sharing nudes – it may be a sexual exploration scenario or it may be due to coercion. It is important to remember that it won't always be appropriate to inform the police; this will depend on the nature of the incident (see **Appendix 1** for definitions).

However, as a school it is important that incidents are consistently recorded. It may also be necessary to assist the young person in removing the image from a website or elsewhere.

If indecent images of a young person are found:

- Act in accordance with the Safeguarding policy i.e. inform the DSL or Deputy
- Store the device securely
- The DSL will assist SLT to carry out a risk assessment in relation to the young person
- The DSL will make a referral

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

Reporting misuse

Misuse by pupils:

- Teachers have the power to discipline pupils 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 pupil 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 pupil is found to be accessing extremist material, shall be dealt with in accordance with our **Safeguarding and Child Protection Policy.**

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.

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 child protection procedures. Pupils and parents will be informed of the complaints procedure.

Monitoring and review

This policy will also be reviewed annually by the **Trust DSL**, 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/pupils.

This policy will be reviewed in **September 2024.**

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.