DIGITAL SAFEGUARDING POLICY

September 2019

Date for Review: September 2020

James Montgomery Academy Trust

Statement of Intent

At the **James Montgomery Academy Trust** 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.
Whilst the academy recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.
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.
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.

Legal framework

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

- 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 (2019) 'Keeping children safe in education'
- Prevent Guidance for schools 2015

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

- Safer Working Practices (May 2019) – 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.

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
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- 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, digital microscopes 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 harm or embarrass another person.
- No portable equipment or devices will be used to bully or intimidate 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 the academy premises.
- No files should be transported off the academy 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 academy site should be encrypted and should only be accessible using a 'strong' password.

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 academy is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard pupils.

The **E-safety Officer** in each school in the academy is responsible for ensuring the day-to-day e-safety in JMAT schools, and managing any issues that may arise.

The JMAT **Board of Directors and CEO** are responsible for ensuring that the **E-safety officers** and any other relevant staff receive CPD to allow them to fulfil their role and train other members of staff.

The **E-safety officer** in each school in the academy will provide all relevant training and advice for members of staff on e-safety as part of the requirement for staff to undergo regularly updated safeguarding training and be able to teach pupils about online safety.

The **JMAT Board of Directors** will ensure there is a system in place which monitors and supports the **E-safety officer**, whose role is to carry out the monitoring of e-safety in JMAT schools, keeping in mind data protection requirements.

The school's **E-safety officer** will regularly monitor the provision of e-safety in the JMAT schools and will provide feedback.

The school's **E-Safety Officer** will establish a procedure for reporting incidents and inappropriate internet use, either by pupils or staff.

Headteacher/Head of School is responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.

All JMAT staff are responsible for ensuring they are up-to-date with current e-safety issues, and this Digital Safeguarding Policy.

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

The **Head of School/Headteacher** is responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.

E-safety control measures

Educating pupils:
Pupils will be taught about the importance of e-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 e-safety training on a regular basis to ensure they are aware of current e-safety issues and any changes to the provision of e-safety, as well as current developments in social media and the internet as a whole.
All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.
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.
Any new staff are required to undergo e-safety training as part of their induction programme, ensuring they fully understand this Digital Safeguarding Policy.

Internet access:
Management systems will be in place to allow teachers and members of staff to control workstations and monitor pupils' activity.
Effective filtering systems will be established to eradicate any potential risks to pupil's inappropriate material.
Filtering systems will be used which are relevant to pupils' age ranges, their frequency of use of IT systems, and the proportionality of costs compared to risks.
The school's **E-Safety Officer** 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 **Head of School/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.
The master users' passwords will be available to the **Head of School/Headteacher** for regular monitoring of activity.
Staff are able to use the internet for personal use during out-of-school hours, as well as break and lunch times.
Personal use will only be monitored by the **E-safety officer** in each school for access to any inappropriate or explicit sites, where it is justifiable to be necessary and in doing so, would outweigh the need for privacy.
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 **Head of School/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 **Head of School/Headteacher** prior to accessing the social media site.

Published content on the JMAT website and images:
The **CEO** will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate.
Contact details on the JMAT website will include the phone number, email and address of the JMAT. 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.
Pupils are not permitted to take or publish photos of others without permission from the individual.
Staff are able to take images, though they must do so in accordance with school policies in terms of the sharing and distribution of such. Staff will not take images using their personal equipment.
Any member of staff that is representing the JMAT online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputability.

Mobile devices and hand-held computers:
Mobile devices are not permitted to be used during school hours by pupils.

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.

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 school **E-safety officer** when using these on JMAT premises.

The sending of inappropriate messages or images from mobile devices is prohibited.

Mobile devices will not be used to take images or videos of pupils or staff.

The JMAT will be especially alert to instances of cyber bullying and will treat such instances as a matter of high priority.

Virus management

Technical security features, such as virus software, are kept up-to-date and managed by the school **E-safety officer**.

The **E-safety officer** in each school in the academy 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

For the purpose of this policy, "cyber bullying" 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 cyber bullying and will commit to preventing any instances that should occur.

Schools in the JMAT will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.

Pupils will be educated about online safety through teaching and learning opportunities as part of a broad and balanced curriculum; this includes covering relevant issues within PSHE lessons as well as sex and relationship education.

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 any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our **Anti-Bullying and Harassment Policy**.

Youth Produced Sexual Imagery (YPSI) – 'sexting'

'Sexting' 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 for the purposes of this policy sexting 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 young people and/or adults via a mobile phone, handheld device, computer, 'tablet' or website with people they may not even know.

Procedure to follow in the event of a YPSI/ 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).**

YPSI/Sexting disclosures should follow the normal safeguarding practices and protocols (see Safeguarding Policy).

Upskirting

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 viewing their genitals or buttocks**.**

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 **Head of School/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 Safeguarding Team 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/sexting – 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 Safeguarding Team
- Store the device securely
- The Safeguarding Team will assist the Guidance/Pastoral team to carry out a risk assessment in relation to the young person
- The Safeguarding Team will make a referral

See Appendix 1 for further information on YPSI/Sexting 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.
Members of staff may decide to issue other forms of disciplinary action to a pupil upon the misuse of the internet. This will be discussed with the **Head of School/Headteacher** and will be issued once the pupil is on the school premises.
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 Policy.**

Misuse by staff:

Any misuse of the internet by a member of staff should be immediately reported to the **Head of School/Headteacher.**
The **Headteacher/Head of School** 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 **Head of School/Headteacher** will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff.

Handling e-safety complaints

Complaints of Internet misuse will be dealt with initially by the **Headteacher/Head of School.**
Any complaint about staff misuse must be referred to the **JMAT CEO/DSL.**
Complaints of a child protection nature must be dealt with in accordance with academy 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 DSL and Safeguarding Director; any changes made to this policy will be communicated to all members of staff.

The review will take into account the following:

- new legislation and government guidance
- previously reported incidents to improve procedures
- latest developments in ICT
- feedback from staff/pupils.

This policy will be reviewed in **September 2020.**

APPENDIX 1

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.