ESPRIT MAGIC

ESPRIT

MULTI ACADEMY TRUST

On Line Teaching Policy

Committee approved on	
Next Review Date: **Updated/Reviewed on**	

Online Teaching Policy

The way schools and colleges are currently operating in response to coronavirus (COVID-19) is fundamentally different to business as usual, however, a number of important safeguarding principles remain the same:

- with regard to safeguarding, the best interests of children must always continue to come first
- if anyone in a school or college has a safeguarding concern about any child they should continue to act and act immediately
- a DSL or deputy should be available at all times, either in person, by video or phone
- it is essential that unsuitable people are not allowed to enter the children's workforce and/or gain access to children
- children should continue to be protected when they are online

It will be more important than ever that schools and colleges provide a safe environment, including online. The Academies will:

- continue to ensure that appropriate filters and monitoring systems are in place to protect children when they are online on the Academy's IT systems or recommended resources
- consider who in their institution has the technical knowledge to maintain safe IT arrangements and should also consider what their contingency arrangements are if their IT staff become unavailable
- take a MAT approach to safeguarding. This will allow us to satisfy ourselves that any new policies and processes in response to COVID-19 are not weakening our approach to safeguarding or undermining our child protection policy.

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

Scope of the Policy

The Education and Inspections Act 2006 empowers Headteachers/Principals to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the trust site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the trust, but is linked to membership of the trust. The 2011 Education Act increased these powers with regard to the searching for and use of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The MAT will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the MAT:

Principal and Senior Leaders

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.
- The Principal and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant MAT disciplinary procedures).

- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead

Online Safety Lead

Are responsible for ensuring that:

- leads the Online Safety Monitoring
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the MAT
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments – with regard to staff equipment used – Securus is the monitoring system currently used and monitored – however this only applies to staff hardware.
- reports regularly to Senior Leadership Team

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current trust online safety policy and practices
- they report any suspected misuse or problem to the Principal/Senior Leader/Online Safety Lead for investigation/action/sanction –refer to whistle blowing policy.
- all digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems - safeguarding contact for vulnerable families – phone calls, text contacts
- they use agreed learning platforms to provide home based learning – e.g. Purple Mash, Education City, TT Rockstars
- in lessons where internet use is pre-planned students/pupils 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, this also applies to links provided by staff including White Rose Maths, Pearson etc.
  (see additional information for use of digital and video images)
- Any concerns to be logged immediately through CPOMS.

Designated Safeguarding Lead/Designated Person/Officer

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- accessing inappropriate websites
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

Students/Pupils:

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so – this can be through a reporting tool on the website, through CEOP (Child Exploitation and Online Protection) or by use of a WHISPER button on the school website – this allows a concern to be registered by a child, accessed by the named staff member (safeguarding/ e-safety lead) and dealt with accordingly. Pupils should also be taught to report abuse to their parents, carers and teachers.

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. The trust will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school/academy in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images – should only be submitted for social media use without faces on show.
- access to parents' sections of the Learning Platform and on-line student/pupil records
- social media – being mindful of appropriate comments.

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety/digital literacy is therefore an essential part of the MAT's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that students/pupils 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 pupils are allowed to freely search the internet, staff/parents/carers should be vigilant in monitoring the content of the websites the young people visit.
- Children should be provided with individual logins for access to the learning platforms (Purple Mash, Education City, TT Rockstars) – in some cases a parental login is also provided.
- Unless directed to websites, children should be monitored by a suitable adult when accessing the internet.
- Children should be directed to the reporting button (WHISPER) on the website *this hasn't been added yet but allows children to report online safety issues which then goes to the lead in charge for monitoring which will allow the DSL to act accordingly.*

Education – Parents/carers

Some parents and carers may have only a limited understanding of online 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 online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The MAT will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, Learning Platform
- Reference to the relevant web sites/publications

Advice from the Children's commission should be shared with parents and should include the following:

- Advice on setting a safe password for various online accounts.
- Not sharing personal information.
- Not befriending strangers.
- Leaving websites if they make you feel uncomfortable.
- Being open and honest about websites visited and ensuring parents are aware.

- Safe username creation – nothing personal (name, age, location).
- Making video calls safely – using a password to ensure only invited people can join, checking the conversation isn't recorded and blurring the background for privacy settings.
- Ensuring privacy settings and location settings are set up.
- Recognising and avoiding fake news.
- Maintaining a sensible use attitude to the excessive screen usage.
- Share emergency contact details for online safety issues.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The academy 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 pupils 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press – photos sent in by parents are sent with consent that they may be used on social media platforms/ websites with the proviso that faces are not used.
- Staff are allowed to take digital/video images to support educational aims, but must follow MAT policies concerning the sharing, distribution and publication of those images. Those images should only be taken on MAT equipment; the personal equipment of staff should not be used for such purposes. If there is no alternative images MUST be deleted from personal devices immediately once used.
- Care should be taken when taking digital/video images that pupils/staff are appropriately dressed and are not participating in activities that might bring the individuals or the MAT into disrepute:
    - Videos should be taken in an appropriate room
    - Adults should be appropriately dressed
    - Behaving in a professional manner
    - Take account of family members in the background
- Pupils/parents must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs

When using communication technologies, the MAT considers the following as good practice:

- The official MAT email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Parents/ carers of pupils should therefore use only the MAT email service to communicate concerns through the safeguarding@espritmat.org. Staff must use the following to primarily communicate with each other – Teams Outlook 365 and academy email accounts. Other apps such as Whats app may also be used for informal networking between teams.
- Users must immediately report, to the nominated person – in accordance with the MAT policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

- Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) Academy systems. Personal email addresses, text messaging or social media must not be used for these communications. Staff must not reply to parental messages on the academy social media accounts (e.g. Facebook, Twitter) – senior leaders will monitor any such messages. In unprecedented circumstances, such as lockdowns, senior leaders may respond to parent queries on social media.
- Year group email addresses for parents to provide evidence of work during school closure is receipt only with the exception of the safeguarding email account which may require a text/ phone call to deal with issues.
- Some forms of communication such as WHATSAPP should be avoided for professional discussions/ meetings.

When official MAT social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under MAT disciplinary procedures

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from academy and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a MAT context, either because of the age of the users or the nature of those activities. The MAT already has safeguarding procedures in place for reporting any concerning behaviour – reporting using CPOMS.

The MAT believes that the activities referred to in the following section would be inappropriate in an academy context and that users, as defined below, should not engage in these activities in/or outside the academy when using academy equipment or systems. The academy policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 N.B. academies should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)						X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the ~~school/~~academy					X	

Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Using ~~school~~ academy systems to run a private business				X	
Infringing copyright				X	
On-line gaming (educational)					
On-line gaming (non-educational)					
On-line gambling					
On-line shopping/commerce					
File sharing					
Use of social media (other than for Academy pages)					
Use of messaging apps					
Use of video broadcasting e.g. Youtube					

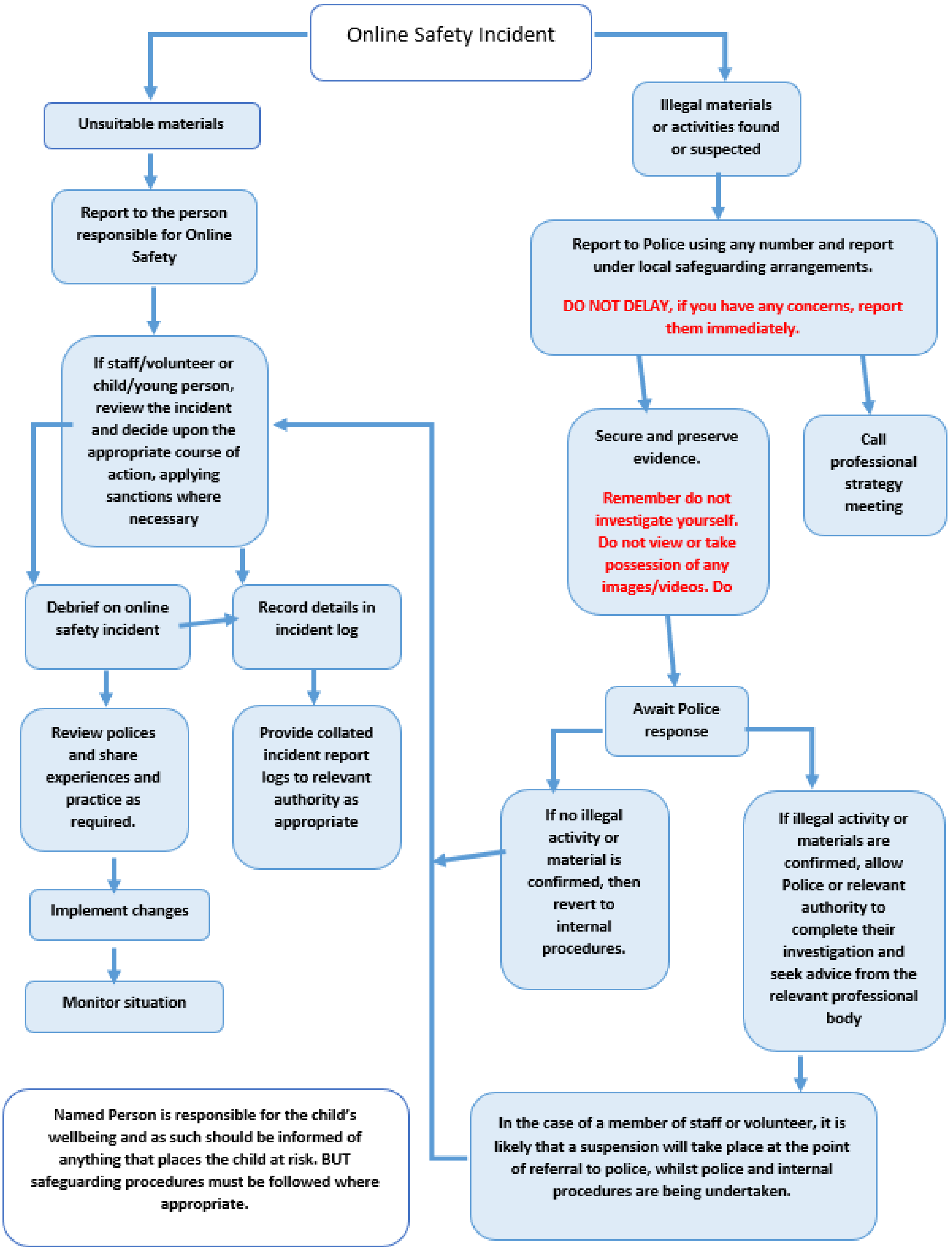
Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.

Responding to incidents of misuse – flow chart



Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.