Stowe Valley
MULTI ACADEMY TRUST

Online Safety Policy

Approved by:		**Date:** 22 May 2019
Last reviewed on:	May 19	
Next review due by:	May 20	

Contents

NOTE: All references to SVMAT Trustees also include SVMAT Members

What is this policy?

Online safety is an integral part of safeguarding. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2018 (KCSIE) and other statutory documents. Any issues and concerns with online safety must follow the SVMAT/School's safeguarding and child protection procedures.

Who is it for; when is it reviewed?

This policy is a living document, subject to full annual review but also amended where necessary during the year in response to developments in our school's local areas and the wider Trust.

This policy is intended for SVMAT/School Staff/Pupils/Parents/Trustees/Local Governing Body Governors.

Who is in charge of online safety?

The Trust's individual school's designated safeguarding leads (DSL) takes lead responsibility for safeguarding and child protection (including online safety). They as a group contribute to this policy.

What are the main online safety risks today?

Online-safety risks are traditionally categorised as one of the 3 Cs: Content, Contact or Conduct (identified by Professor Tanya Byron's 2008 report "Safer children in a digital world"). These three areas remain a helpful way to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all three.

For many years, online-safety messages have focussed on 'stranger danger', i.e. meeting strangers online and then meeting them face to face (contact). Whilst these dangers have not gone away and remain important, violent or sexual content is now prevalent – sending or receiving, voluntarily or coerced. Examples of this are sexting, the sharing of violent and sexual videos, self-harm materials, coerced nudity via live streaming, Cyber Bullying, peer-on-peer sexual exploitation, child criminal exploitation and radicalisation. Contact and conduct of course also remain important challenges to address.

How will this policy be communicated?

This policy can only impact upon practice if it is a (regularly updated) living document. It must be accessible to and understood by all stakeholders. It will be communicated in the following ways:

- Posted on the SVMAT/School website
- Available on the internal staff network
- Available in paper format in the policies folder
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff)
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers (which must be in accessible language appropriate to these groups).
- AUPs issued to whole school community, on entry to the school, with annual reminders of where to find them if unchanged, and reissued if updated after annual review
- AUPs are displayed in appropriate classrooms/corridors (not just in Computing corridors/classrooms)
- Reviews of this online-safety policy will include input from staff, pupils and other stakeholders, helping to ensure further engagement

1. Aims

Our Trust aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Set out expectations for all Stowe Valley Multi-Academy Trust community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help Trust staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the SVMAT/School, supporting the SVMAT/School ethos, aims and objectives, and protecting the reputation of the SVMAT/School and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other SVMAT/School policies such as Behaviour Policy or Anti-Bullying Policy)

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation and the guidance on sexting.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The Trust Board

The Trust Board has overall responsibility for monitoring this policy and holding the CEO/Headteachers to account for its implementation.

The Local Governing Bodies are responsible for monitoring and the implementation of this policy at a local school level, they will also co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All Trustees and Local Governing Body Members will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the SVMAT/School's ICT systems and the internet

3.2 The CEO/Headteachers

The CEO/Headteachers are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the SVMAT/School.

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into Trust-wide/whole-school safeguarding
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance
- Liaise with the designated safeguarding leads on all online-safety issues which might arise and receive regular updates on SVMAT/School issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the SVMAT/School's provision follows best practice in information handling; work with the DPO, DSL, Trustees and LGB Governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure the SVMAT/School implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets the needs of pupils, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures
- Ensure Trustees and LGB Governors are regularly updated on the nature and effectiveness of the SVMAT/School's arrangements for online safety
- Ensure the SVMAT/School website meets statutory DfE requirements (see appendices for website audit document)

3.3 The designated safeguarding lead

Details of the SVMAT/School's designated safeguarding lead (DSL) are set out each schools' child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in each MAT school, in particular:

- Supporting the CEO/Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the MAT
- Working with the CEO/Headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the CEO, Headteacher and/or Trustees and Local Governing Board Governors.
- "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)."
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Ensure "An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- "Liaise with the local authority and work with other agencies in line with Working together to safeguard children"
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Work with the CEO, Headteacher, DPO, Trustees and Local Governing Body Governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safety
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the Trust Board.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends
- Ensure that online safety education is embedded across the curriculum and beyond, in wider school life
- Promote an awareness and commitment to online safety throughout the MAT community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents
- Liaise with school technical, pastoral, and support staff as appropriate
- Communicate regularly with SLT and the designated Safeguarding Local Governing Body Governor to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- Oversee and discuss 'appropriate filtering and monitoring' with Trustees and Local Governing Body Governors and ensure staff are aware.
- Ensure the 2018 Department for Education guidance on sexual violence and harassment is followed throughout the MAT and that staff adopt a zero-tolerance approach to this, as well as to bullying

- Facilitate training and advice for all staff:
  - all staff must read KCSIE Part 1 and all those working with children Annex A as well as an awareness of Annex C (Online Safety)
  - cascade knowledge of risks and opportunities throughout the organisation
  - See cpd.lgfl.net for useful materials including PowerPoints, videos and more

This list is not intended to be exhaustive.

3.4 The ICT Director

The ICT Director is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at SVMAT/School, including terrorist and extremist material
- Ensuring that the MAT School's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the MAT School's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the SVMAT/School behaviour policy
- Keep up to date with the SVMAT/School's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the designated safeguarding lead / online safety lead / data protection officer to ensure that SVMAT School systems and networks reflect SVMAT policy
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc.
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the ICT Director and local DSL/senior leadership team
- Maintain up-to-date documentation of the SVMAT's online security and technical procedures
- To report online-safety related issues that come to their attention in line with SVMAT policy
- Manage the SVMAT's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy

- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the SVMAT ICT systems and the internet (appendix 2), and ensuring that pupils follow the SVMAT's terms on acceptable use (appendix 1)
- Working with their individual Trust School's DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the SVMAT/School behaviour policy
- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Leads (DSL) and Online Safety Leads (OSL) are
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for SLT and those working directly with children, it is good practice for all staff to read all three sections).
- Read and follow this policy in conjunction with the SVMAT/School's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with SVMAT/School procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the staff acceptable use policy and code of conduct.
- Notify the DSL/OSL if policy does not reflect practice in your SVMAT/School and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all SVMAT/School activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc.) in SVMAT/School or setting as homework tasks, encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites.
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended SVMAT/School activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law
- Encourage pupils to follow their acceptable use policy, remind them about it and enforce SVMAT/School sanctions
- Notify the DSL/OSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/OSL know
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safety issues
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the SVMAT/School hours and site, and on social media, in all aspects upholding the reputation of the Trust and of the professional reputation of all staff.

This list is not intended to be exhaustive.

3.6 Pupils

Throughout the course of a pupil's time within the Trust's schools, Pupils will be taught about online safety as part of the curriculum:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns
- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns?

The safe use of social media and the internet will also be covered in other subjects where relevant.

The SVMAT School's will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Key responsibilities:

- Read, understand, sign and adhere to the pupil acceptable use policy and review this annually
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of School and realise that the SVMAT/School's acceptable use policies cover actions out of School, including on social media
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

3.7 Parents

SVMAT recognise the crucial role that Parents play with regards to the safety of our pupils. Parents are therefore encouraged to:

- Notify a member of Teaching/Admin staff or the individual school Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the SVMAT/School's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

The SVMAT/School will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the respective Headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of teaching/admin staff or the Headteacher.

Key responsibilities:

- Read, sign and promote the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it
- Consult with the school if they have any concerns about their children's use of technology
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the SVMAT/School staff, volunteers, governors, contractors, pupils or other parents/carers.

3.8 Visitors and members of the community

Visitors and members of the community who use the SVMAT/School's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

3.9 External groups including parent associations

Staff or SVMAT representatives booking any access to SVMAT buildings/facilities for individuals or groups must insure that the following responsibilities are met

Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school .It is the schools responsibility to ensure that this happens.
- Support the SVMAT/School in promoting online safety and data protection
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the SVMAT/School staff, volunteers, governors, contractors, pupils or other parents/carers

3.10 Data Protection Officer (DPO)

SVMAT contract the Warwickshire Local Authority Schools Legal Services Data Protection Officer Service as their Data Protection Officer (DPO). The SVMAT will ensure that the arrangement and/or contract reflects our responsibilities under this E-Safety Policy.

Key responsibilities:

- Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (April 2018), especially this quote from the latter document:
    - GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between SVMAT/Schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards should still be in place [...] Remember, the law does not prevent information about children being shared with specific authorities if it is for the purposes of safeguarding
- The same document states that the retention schedule for safeguarding records may be required to be set as 'Very long term need (until pupil is aged 25 or older)'
- Work with the DSL, CEO/Headteacher, Trust Board and local governing bodies to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

4. Education and curriculum

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- PSHE
- Health Education, Relationships (in secondaries: Relationships and Sex) Education (being implemented from September 2019 for September 2020)
- Computing
- Citizenship

However, as stated in the role descriptors above, it is the role of all Trust staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc.) in any of the Trust's schools or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your individual school DSL what appropriate filtering and monitoring policies are in place).

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

At Stowe Valley Multi Academy Trust we recognise that online safety and broader digital resilience must be thread throughout the curriculum.

5. Handling online-safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE, Citizenship and (from September 2019 for September 2020) the new statutory Health Education and Relationships Education (for secondaries: Relationships and Sex Education).

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the online-safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

Non-teaching staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

SVMAT/School procedures for dealing with online-safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

The Trust commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on pupils when they come into school. All members of the SVMAT/School are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about SVMAT/School staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of the Local Governing Body and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

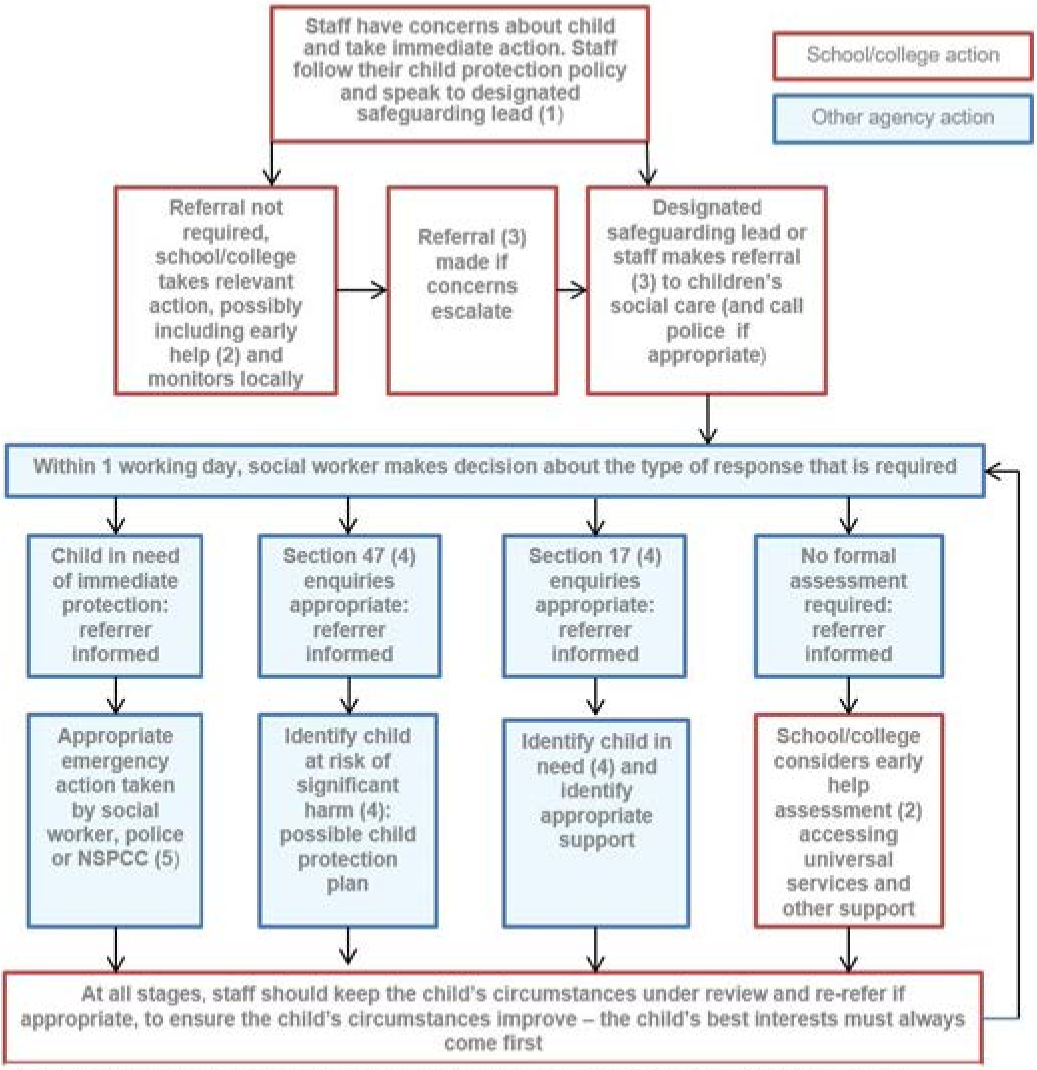
Any concern/allegation about SVMAT core staff misuse must be referred directly to the CEO, unless the concern is about the CEO in which case the complaint is referred to the Chair of the SVMAT Trust Board.

The SVMAT will actively seek support from other agencies as needed (i.e. the local authority, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sexting; see section below).

5.1 Actions where there are concerns about a child

As outlined previously, online safety concerns are no different to any other safeguarding concern.

Staff with concerns about a child's safety should refer to the Trust's Safeguarding Policy. The flowchart below, taken from page 13 of Keeping Children Safe in Education 2018 as the key education safeguarding document and provides an overview of the process.


Staff have concerns about child and take immediate action. Staff follow their child protection policy and speak to designated safeguarding lead (1)
School/college action
Other agency action
Referral not required, school/college takes relevant action, possibly including early help (2) and monitors locally
Referral (3) made if concerns escalate
Designated safeguarding lead or staff makes referral (3) to children's social care (and call police if appropriate)
Within 1 working day, social worker makes decision about the type of response that is required
Child in need of immediate protection: referrer informed
Section 47 (4) enquiries appropriate: referrer informed
Section 17 (4) enquiries appropriate: referrer informed
No formal assessment required: referrer informed
Appropriate emergency action taken by social worker, police or NSPCC (5)
Identify child at risk of significant harm (4): possible child protection plan
Identify child in need (4) and identify appropriate support
School/college considers early help assessment (2) accessing universal services and other support
At all stages, staff should keep the child's circumstances under review and re-refer if appropriate, to ensure the child's circumstances improve – the child's best interests must always come first

(1) In cases which also involve an allegation of abuse against a staff member, see Part Four of this guidance.

(2) Early help means providing support as soon as a problem emerges at any point in a child's life. Where a child would benefit from co-ordinated early help, an early help inter-agency assessment should be arranged. Chapter one of Working together to safeguard children provides detailed guidance on the early help process.

(3) Referrals should follow the local authority's referral process. Chapter one of Working together to safeguard children.

(4) Under the Children Act 1989, local authorities are required to provide services for children in need for the purposes of safeguarding and promoting their welfare. This can include section 17 assessments of children in need and section 47 assessments of children at risk of significant harm. Full details are in Chapter One of Working together to safeguard children.

(5) This could include applying for an Emergency Protection Order (EPO).

5.2 Sexting

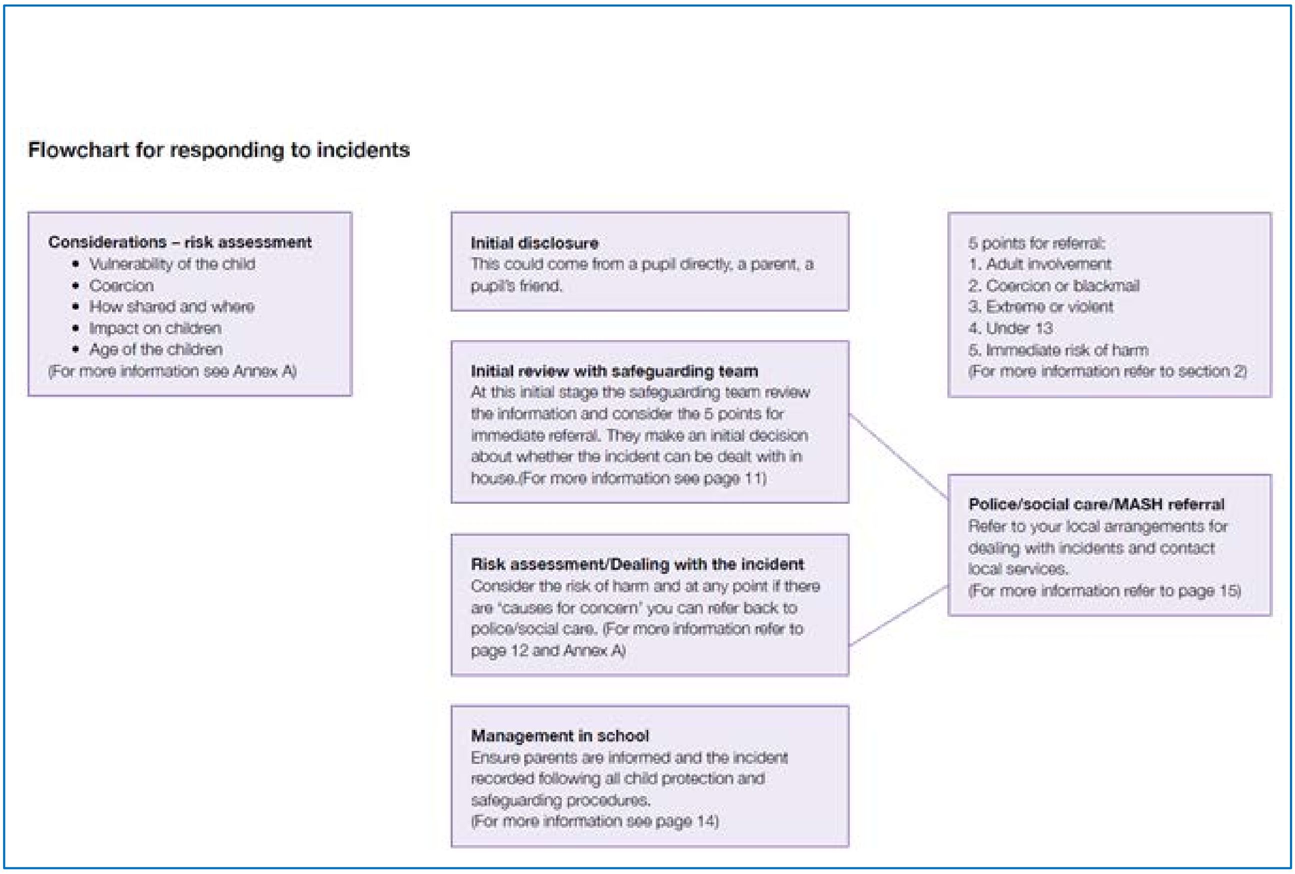
All SVMAT Schools (regardless of phase) should refer to the UK Council for Child Internet Safety (UKCCIS) guidance on sexting (also referred to as 'youth produced sexual imagery') in schools. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse, Government guidance on Sexting in schools and colleges is available here.

There is a one-page overview for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

The school DSL will in turn use the full 50-page guidance document including case studies, typologies and a flow chart as shown below (for information only, must be viewed in the context of the full document) to decide next steps and whether other agencies need to be involved.

It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

The documents referenced above and materials to support teaching about sexting can be found at sexting.lgfl.net .



Flowchart for responding to incidents

Considerations – risk assessment
- Vulnerability of the child
- Coercion
- How shared and where
- Impact on children
- Age of the children

(For more information see Annex A)

Initial disclosure
This could come from a pupil directly, a parent, a pupil's friend.

Initial review with safeguarding team
At this initial stage the safeguarding team review the information and consider the 5 points for immediate referral. They make an initial decision about whether the incident can be dealt with in house.(For more information see page 11)

Risk assessment/Dealing with the incident
Consider the risk of harm and at any point if there are 'causes for concern' you can refer back to police/social care. (For more information refer to page 12 and Annex A)

Management in school
Ensure parents are informed and the incident recorded following all child protection and safeguarding procedures.
(For more information see page 14)

5 points for referral:
1. Adult involvement
2. Coercion or blackmail
3. Extreme or violent
4. Under 13
5. Immediate risk of harm

(For more information refer to section 2)

Police/social care/MASH referral
Refer to your local arrangements for dealing with incidents and contact local services.
(For more information refer to page 15)

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the SVMAT Behaviour Policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, The Trust will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. The Trust will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The SVMAT Schools will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, Trustees, Local Governing Body Governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The SVMAT Schools also send information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the SVMAT School will follow the processes set out in the SVMAT/School Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the SVMAT/School will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

SVMAT/School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of SVMAT/School discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the SVMAT complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers, Trustees and Local Governing Body Governors are expected to sign an agreement regarding the acceptable use of the SVMAT/School's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the SVMAT/School's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

SVMAT will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Staff using work devices outside school

Staff members using a work device outside their place of work must not install any unauthorised software on the device and must not use the device in any way which would violate the SVMAT terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside their place of work. Any USB devices containing data relating to the SVMAT/School must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT Manager/Trust ICT Director.

Work devices must be used solely for work activities.

9. Sexual violence and harassment

In 2018 new Department for Education guidance was issued on sexual violence and harassment, as a new section within Keeping Children Safe in Education and also a document in its own right. It would be useful for all staff to be aware of the DfE guidance: paragraphs 45-49 cover the immediate response to a report and confidentiality which is highly relevant for all staff; the case studies section provides a helpful overview of some of the issues which may arise.

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

The following is an excerpt from section 46 on page 21 of that document:

"As with all safeguarding concerns, it is important that in such instances staff take appropriate action in accordance with their child protection policy. They should not assume that someone else is responding to any incident or concern. If in any doubt, they should speak to the designated safeguarding lead (or a deputy). In such cases, the basic safeguarding principles remain the same, but it is important for the school or college to understand why the victim has chosen not to make a report themselves. This discussion should be handled sensitively and with the support of children's social care if required. There may be reports where the alleged sexual violence or sexual harassment involves pupils or students from the same school or college, but is alleged to have taken place away from the school or college premises, or online. There may also be reports where the children concerned attend two or more different schools or colleges. The safeguarding principles, and individual schools' and colleges' duties to safeguard and promote the welfare of their pupils and students, remain the same. The same principles and processes as set out from paragraph 48 will apply. In such circumstances, appropriate information sharing and effective multi-agency working will be especially important."

10. Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of the Trust's school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on and outside of school site).

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of SVMAT/School platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy.

Where pupils contravene these rules, the SVMAT/School Behaviour Policy will be applied; where staff contravene these rules, action will be taken as outlined in the Staff Code of Conduct

Further to these steps, SVNAT reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto SVMAT property.

11. Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the Trust and its constituent schools. These are also governed by school Acceptable Use Policies.

Breaches will be dealt with in line with the School Behaviour Policy (for pupils) or Code of Conduct.

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, The Trust or one of its constituent Schools will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, SVMAT or the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process.

12. Data protection and data security

This section serves to highlight general principles regarding the relationship between safeguarding and data protection / data security, and to signpost to useful information.

There are references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (April 2018), which the DPO and DSL will seek to apply. This quote from the latter document is useful for all staff – note the red and purple highlights:

"GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, **appropriate organisational and technical safeguards should still be in place [...]** Remember, **the law does not prevent information about children being shared with specific authorities if it is for the purposes of safeguarding**."

All pupils, staff, Trustees and Local Governing Body Governors, volunteers, contractors and parents are bound by the SVMAT/School's data protection policy and agreements.

The CEO/Headteacher, data protection officer, Trustees and Local Governing Body Gvernors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions.

12.1 Appropriate filtering and monitoring

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

12.2 Electronic communications

Please read this section alongside references to pupil-staff communications in the overall SVMAT/School Safeguarding Policy, and in conjunction with the Data Protection Policy. This section only covers electronic communications, but the same principles of transparency, appropriate conduct and audit trail apply.

12.3 Email

Currently across the Trust school's we use a mixture of the following email systems for all Trustees, Local Governing Body Governors, Staff and Pupils.

- Warwickshire LA WeLearn365 system
- On-Premise Microsoft Exchange and Office 365
- Gmail

Both these systems are linked to an authentication system and are fully auditable, trackable and managed on behalf of the Trust's school. This is for the mutual protection and privacy of all Trustees, Local Governing Body Governors, Staff, Pupils and parents, as well as to support data protection.

General principles for email use are as follows:

Email is the only means of electronic communication to be used between staff and pupils / staff and parents (in both directions). Use of a different platform must be approved in advance by the CEO/Headteacher in advance. Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the CEO/Headteacher (if by a staff member).

Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the CEO/Headteacher should be informed immediately.

Staff or pupil personal data should never be sent/shared/stored on email.

Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the SVMAT/School into disrepute or compromise the professionalism of staff

Staff are allowed to use the email system for reasonable (not excessive, not during lessons) personal use but should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.

See also the social media section of this policy (Section 15.)

12.4 School website

The SVMAT and School websites are a key public-facing information portal for the school communities (both existing and prospective stakeholders) with a key reputational value. The sites are managed by the Trust's Media Manager.

The Department for Education has determined information which must be available on a school website.

Where other staff submit information for the website, they are asked to remember:

SVMAT has the same duty as any person or organisation to respect and uphold copyright law – SVMAT/Schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission. There are many open-access libraries of high-quality public-domain images that can be used (e.g. pixabay.com for marketing materials – beware some adult content on this site).

Where pupil work, images or videos are published on the website, their identities are protected and full names are not published (remember also not to save images with a filename that includes a pupil's full name).

12.5 Cloud platforms

Many schools are recognising the benefits of cloud computing platforms, not just for cost savings but to enhance teaching and learning.

The Trust and its schools adhere to the principles of the Department for Education document 'Cloud computing services: guidance for school leaders, school staff and governing bodies'.

As more and more systems move to the cloud, it becomes easier to share and access data. It is important to consider data protection before adopting a cloud platform or service – Microsoft's Office 365

For online safety, basic rules of good password hygiene ("Treat your password like your toothbrush –never share it with anyone!"), expert administration and training can help to keep staff and pupils safe, and to avoid incidents. The CEO/Headteacher analyses and documents systems and procedures before they are implemented, and regularly review them.

The following principles apply:

- Privacy statements inform parents and children (13+) when and what sort of data is stored in the cloud
- The DPO approves new cloud systems, what may or may not be stored in them and by whom.
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Two-factor authentication is used for access to staff or pupil data
- Pupil images/videos are only made public with parental permission
- Only SVMAT/School-approved platforms are used by students or staff to store pupil work
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain)

12.6 Digital images and video

When a pupil/student joins a SVMAT School, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos and for what purpose (beyond internal assessment, which does not require express consent). Parents answer as follows:

- For displays around the school
- For the newsletter
- For use in paper-based school marketing
- For online prospectus or websites
- For a specific high profile image for display or publication
- For social media

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.

Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At any of the Trust's Schools no member of staff will ever use their personal phone to capture photos or videos of pupils.

Photos are stored on the SVMAT networks in line with the retention schedule of the SVMAT Data Protection Policy.

Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children

Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

13. Social media

13.1 Trust and individual School's Social Media presence

Stowe Valley Multi Academy Trust and its constituent Schools work on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first 'googling' the school.

Negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online Safety Helpline (POSH: helpline@saferinternet.org.uk) involve schools' (and staff members') online reputation.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

The CEO/Headeacher/appointed Staff Member is responsible for managing individual schools Facebook/Twitter etc. account(s).

13.2 Staff, pupils' and parents' SM presence

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a MAT, we accept that many Trustees, Local Governing Body Governors, Staff, Pupils and Parents will use it. However, as stated in the acceptable use policies which all members of the SVMAT community sign, we expect everybody to behave in a positive manner, engaging respectfully with the SVMAT/School and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the SVMAT/School or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the SVMAT/Individual School, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the SVMAT/School Complaints Procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the SVMAT/School (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13, but the SVMAT schools regularly deal with issues arising on social media with pupils under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that following on from the government's Safer Internet Strategy, enforcement and age checking is likely to become more stringent over the coming years.

However, the SVMAT/School has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

The Trust and its schools have an official Facebook managed by the CEO/Headeacher/appointed Staff Member and will respond to general enquiries about the SVMAT/School, but asks parents/carers not to use these channels to communicate about their children.

- Email is the official electronic communication channel between parents and the school, and between staff and pupils.

Pupils are not allowed* to be 'friends' with or make a friend request** to any staff, Trustees/Local Governing Body Governors, volunteers and contractors or otherwise communicate via social media.

Pupils are discouraged from 'following' staff, Trustees, Local Governing Body Governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the CEO/Headteacher, and should be declared upon entry of the pupil or staff member to the school).

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the CEO/Headteacher (if by a staff member).

Staff are reminded that they are obliged not to bring the SVMAT/School or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the SVMAT/School or its stakeholders on social media and be careful that their personal opinions might not be attributed to the SVMAT/School or local authority, bringing the SVMAT/School into disrepute.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that of the 131 Prohibition Orders issued to staff in 2017, 73 involved social media/technology (and 27 of the 66 orders by August 2018).

All members of the SVMAT/School community are reminded that particularly in the context of social media, it is important to comply with the SVMAT and individual school's policy on Digital Images and Video and permission is sought before uploading photographs, videos or any other information about other people.

14. Device usage

Please read the following in conjunction with acceptable use policies and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

14.1 Personal devices and bring your own device (BYOD) policy

Pupils in year 6 and above are allowed to bring mobile phones in for emergency use only.

- In the case of Primary School Pupils - Phones are handed in to the school office in the morning and collected at the end of the day. The SVMAT/School takes no responsibility for these items.

- In the case of Secondary School Pupils – Phone are not to be used on school premises

All staff who work directly with children should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the Digital images and video section and Data protection and data security section. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.

Volunteers, contractors, Trustees and Local Governing Body Governors should leave their phones in their pockets and on silent. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the CEO/Individual School Headteacher should be sought (the CEO/Headteacher may choose to delegate this) and this should be done in the presence of a member staff.

14.2 Network / internet access on school devices

Pupils are not allowed networked file access via personal devices. However, they are allowed to access the school wireless internet network for school-related internet use within the framework of the acceptable use policy. All such use is monitored.

All staff who work directly with children should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the Digital images and video section and Data protection and data security section of this document. Child/staff data should never be downloaded onto a private phone.

Volunteers, contractors, Trustees and Local Governing Body Governors can access the guest wireless network but have no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored.

Parents have no access to the school network or wireless internet on personal devices

15. Trips / events away from school

For school trips/events away from school, teachers will be issued a school duty phone and this number used for any authorised or emergency communications with pupils/students and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the CEO/Headteacher. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

16. Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Trust CEO/School Headteachers and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

17. How the SVMAT/School will respond to issues of misuse

Where a pupil misuses the SVMAT/School's ICT systems or internet, the SVMAT/School will follow the procedures set out in the Behaviour Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the SVMAT/School's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The SVMAT/School will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

18. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

Each DSL and/or Deputy will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Trustees/Local Governing Body Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

19. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

This policy will be reviewed annually by the Trust's Director of ICT at every review, the policy will be shared with the Trust Board.

20. Links with other policies

This Online Safety Policy is linked to our:

- Child Protection and Safeguarding Policy at each MAT School
- Behaviour Policy
- Staff disciplinary procedures
- Data Protection Policy and Privacy notices
- Complaints procedure

Appendix 1: acceptable use agreement (pupils and parents/carers)

Acceptable use of the SVMAT/School's ICT systems and internet: agreement for pupils and parents/carers

Name of pupil:

ICT and the related technologies such as the internet and email are an important part of learning in our SVMAT/School.

We expect all Students to be responsible for their behaviour when using ICT and the Internet. It is essential that Students are aware of e-Safety and know how to stay safe when using any ICT.

Students are expected to discuss this policy with their parent or guardian and then to sign and follow the e-Safety Rules. Any concerns or explanation can be discussed with their class teacher or the e-Safety coordinator.

No student will have access to the internet unless they have returned a signed form, without exception. Any student who is subsequently disciplined for misuse of their network account, Internet or email privilege with have their access withdrawn in accordance with the school's e-safety policy. Parents will be informed of the nature of the offence, and Internet/email access may in some cases only be returned once the school and parents have agreed and a further consent form has been returned.

- I will only use the SVMAT/School's ICT systems including the internet, email, digital video etc for school purposes, and only when under the supervision of a member of staff.
- I will not attempt to download or install software on SVMAT/School technologies.
- I will only access the SVMAT/School network using my own user name and password and will not access any other user's files – If someone else finds out my password I will change it immediately.
- I will follow the SVMAT/School's ICT security system and not reveal my passwords to anyone, I will change my password regularly.
- I will not bring in any viruses or malicious programs using USB sticks or other removable media. I will ensure any files I bring to school are virus scanned before connecting them to the SVMAT/School network(s).
- I will only use my SVMAT/School email address for email communication between other students and staff.
- I will access any not non-SVMAT/School email accounts though the school network, such as Hotmail and Yahoo Mail.
- I will make sure that all ICT communications with Students, teachers or others is responsible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download or upload material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher or another member of staff.

- I will not send to Students, teachers or others material that could be considered offensive or illegal.
- I will not upload content to the SVMAT/School VLE (Where available) that may be offensive, or hurtful to any member of the SVMAT/School community.
- I will not complete and send on-line forms without the permission from my teacher.
- I will not give out any personal information such as name, phone number or address. I will not use the SVMAT/School ICT systems to arrange to meet someone unless this is part of a school project approved by my teacher.
- I will not attempt to bypass the SVMAT/School internet filtering system.
- Images of pupils and/ or staff will only be taken, stored and used for SVMAT/School purposes in line with SVMAT/School policy and not be distributed outside the SVMAT/School network.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will respect SVMAT/School technologies and understand I may be liable for any damage I cause to SVMAT/School equipment.
- I understand that all my use of the Internet and other related technologies is monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, SVMAT/School sanctions will be applied and my parent/guardian may be contacted.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the SVMAT/School's ICT systems and internet when appropriately supervised by a member of SVMAT/School staff. I agree to the conditions set out above for pupils using the SVMAT/School's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement (Staff, Trustees, Local Governing Body Governors, Volunteers and Visitors)

Acceptable use of the SVMAT/School's ICT systems and the internet: agreement for Staff, Trustees, Local Governing Body Governors, Volunteers and Visitors

Name of Staff member/Trustee/Local Governing Body Governor/Volunteer/Visitor (Delete as Appropriate):

ICT and the related technologies such as email, the internet and mobile phones are an expected part of our daily working life in school.

This policy is designed to ensure that all Staff, Trustees, Local Governing Body Governors, Volunteers and Visitors are aware of their professional responsibilities when using any form of ICT. All Staff, Trustees, Local Governing Body Governors, Volunteers and Visitors are expected to sign this policy and adhere at all times to its contents.

Failure to follow this policy may result in disciplinary or other action in accordance with the SVMAT/School's e-safety policy.

- I will not engage in any activity that is illegal under UK or European law including but not limited to:
  - Copyright Violation
  - Introducing malicious programs into the school network
  - Using school systems to download, store, or distribute illegal software and media
  - Effecting security breaches. Security breaches include but are not limited to: accessing data which I am not the intended recipient; accessing a server or account without express authorisation; enabling another to gain access to data and systems without authorisation.
- I will only use the SVMAT/School's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the CEO/Headteacher, Trust Board or Local Governing Body.
- I will not install software on any SVMAT/School device without authorisation.
- I will not attempt to bypass internet filtering systems or other network security systems.
- I understand that I cannot expect files stored on SVMAT/School servers/platforms or equipment will always be private. Due to the need to protect the SVMAT/School network's the confidentiality of information stored on any device belonging to the SVMAT/School cannot be guaranteed.
- I understand that authorised individuals within the SVMAT/School may monitor equipment, system and network traffic. Any unauthorised files found will be deleted without warning, and use in breach of this agreement will be reported to my line manager.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will only access the computer system with the login and password I have been given
- I will not access other network user's files unless specifically authorized to do so.

- I will ensure that all electronic communications with Students and staff are compatible with my professional role.
- I will only use the approved, secure email system(s) for any SVMAT/School business.
- I will not send to Students or colleagues material that could be considered offensive or illegal
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, or accessed remotely.
- I will not take personal or sensitive data off site on any equipment including computers and removable media unless permission is sought and appropriate encryption is used.
- I will not browse, download or upload material that could be considered offensive or illegal.
- Images of Students will only be taken and used for professional purposes and will not be distributed outside the school network without the permission of the parent/carer.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will support and promote the SVMAT/School’s e-Safety policy and help Students to be safe and responsible in their use of ICT and related technologies.
- I will report any accidental access to inappropriate materials to the appropriate line manager.
- I will ensure all documents are saved, accessed and deleted in accordance with the SVMAT/School’s network security and confidentiality protocols.
- I will not connect a computer or laptop to the SVMAT/School’s network / Internet that does not have up-to-date version of anti-virus software.
- I will not allow unauthorised individuals to access Email / Internet / Intranet.
- I agree and accept that any computer or laptop loaned to me by the SVMAT/School, is provided solely to support my professional responsibilities and that I will notify the school of any “significant personal use” as defined by HM Revenue & Customs.
- I understand any personal blogging, either through SVMAT/School or personal equipment, is subject to the terms and restrictions of this policy. I will not provide pupils with access to personal profiles on social networking sites or add students as “friends”. I will ensure my profiles are “locked down” for my own protection.
- I will not employ any SVMAT/School IT equipment for commercial purposes other than that of approved SVMAT/School business.
- I will immediately report any unauthorised use of SVMAT/School systems or any attempt by an individual, group or third party to breach the SVMAT/School’s security system, whether or not it is successful.
- I will protect the SVMAT/School’s IT equipment. Where damage or loss has occurred I will be liable for the cost of replacement.
- I will report any faults with IT systems to the support desk using the help desk system at the earliest opportunity.
- I will not attempt to alter the configuration or setup of any IT systems without the correct authorisation.
- I understand that failure to comply with the Usage Policy could lead to disciplinary action, or referral to the police in the event of a serious breach.

Signed (staff member/governor/volunteer/visitor):

Date:

Appendix 3: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in the SVMAT/School?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the SVMAT/School's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the SVMAT/School's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the SVMAT/School's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4: online safety incident report log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**