Stowe Valley
MULTI ACADEMY TRUST

Online Safety and Acceptable Use Policy and Guidance

Adopted by Trustees: 20th July 2021

Next Review Date: July 2022

Person responsible for overseeing the implementation: CEO

Chair of Trustees signature: C.L Chevassut

Contents

Glossary

For this document the following terminology should be considered:

Safeguarding and promoting the welfare of children is defined for the purposes of this guidance as:

- protecting children from maltreatment;
- preventing impairment of children's mental and physical health or development;
- ensuring that children grow up in circumstances consistent with the provision of safe and effective care; and
- taking action to enable all children to have the best outcomes.

Child protection refers to the processes undertaken to protect children who have been identified as suffering or being at risk of suffering significant harm.

Staff refers to all those working for or on behalf of the school, full time or part-time, temporary or permanent, in either a paid or voluntary capacity.

Contractor refers to any adult who has been contracted by the Trust, or school, to work with children

DSL refers to the designated safeguarding lead at the School.

Child includes everyone under the age of 18.

SVMAT Trustees also include SVMAT Members

Parent refers to birth parents and other adults who are in a parenting role, for example, stepparents, foster carers and adoptive parents.

Extra familial Harm - Contextual Safeguarding refers to our commitment to understanding wider environmental factors in a child's life that may be a threat to their safety and/or welfare.

Scope of the policy

Online safety is an integral part of safeguarding. Accordingly, this policy is written in line with Keeping Children Safe in Education, DFE, 2021 (KCSIE) and other statutory documents detailed at the end of this policy. Each school has a safeguarding policy, which acts as the sole point of reference when managing a safeguarding concern, this includes concerns that arise from the use of technology in all forms.

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/supply staff/Pupils/Parents/Trustees/Local Governing Body Governors.

The Director of Safeguarding and the ICT Director have strategic oversight of our online safety strategy, however the Trust's individual school's designated safeguarding leads (DSL) taking lead responsibility for safeguarding and child protection (including online safety) within schools.

Each school has a named 'eSafety lead'.

School	eSafety Lead
Bilton School	Claire Harwood
Southam College	Amanda Freemantle
Kineton High School	Mike Few
Southam Primary School	Amanda Startup
Rokeby Primary School	Ian Marks
Temple Herdewyke Primary School	Maggie Godfrey
Bishops Itchington Primary School	Kat Aston
Byfield School	David Hibbert
Stockton Primary School	Anne Bedgood

Each eSafety lead can be contacted through their respective school office.

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 The Trust to protect and educate the whole school community in its use of technology

Establish clear processes 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 (2021), and the documents referenced therein.

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. Their key responsibilities are:

- 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 Partnership
- 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 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 3) 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
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the CEO, Director of Safeguarding, 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 eSafety Lead 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, Director of Safeguarding, Headteacher and/or Trustees and Local Governing Board 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 the Senior Leadership Team 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.
- Facilitate training and advice for all staff

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 3) 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 3) 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

- 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 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)

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. Parents should:

- 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

- 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)

The Head of Governance and Compliance acts as the Data Protection Officer (DPO). The SVMAT will ensure that the arrangement and/or contract reflects our responsibilities under this E-Safety Policy. The key responsibilities of the DPO are to:

- Be aware 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

Each school has a Relationship, Sexual and Health Education Policy. This curriculum is bespoke to each school. The curriculum includes schemes of work around;

- Internet safety and harms
- Online relationships
- Online Media
- Cyber-bullying
- Staying safe online
- Online grooming
- Sexting
- Taking care of myself online.

This list is not exhaustive. Each school has a RSHE Policy published on their school website.

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

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 of 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

Safeguarding concerns will be handled in line with the school safeguarding policy, as published on their school website.

The key principles of that policy, in relation to the reporting of safeguarding concerns are;

- Any safeguarding concerns must be reported immediately to the Designated Safeguarding Lead.
- Concerns about an adult must be reported to the headteacher, concerns about the headteacher must be reported to the Chair of the Governing body.

6. Examining electronic devices

SVMAT/School staff have the specific power under the Education and Inspections Act 2006 (as amended 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, smart watches, where they believe there is a 'good reason' to do so.

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. 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 Trust ICT Director.

Work devices must be used solely for work activities.

If a member of staff believes their data has been shared or accessed, they must inform the Trust Data Protection Officer.

8. Misuse of school technology (devices, systems, networks or platforms) – Pupils and Staff

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.

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

The school will also consider any extra-familiar harm that may be occurring, when addressing misuse of devices, systems, networks or platforms.

9. Social media

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.

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

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.

10 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."

10.1 Email

Currently across the Trust schools 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

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.

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 and non excessive 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.

11. 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.’

Where pupil work, images or videos are published on the website, their identities are protected and full names are not published.

12. Cloud platforms

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.

When using a cloud storage solution, the following principles apply:

- Privacy statements inform parents and children (13+) when and what sort of data is stored in the cloud
- The Director of ICT approves new cloud systems, what may or may not be stored in them and by whom.
- The Head of Governance and Compliance will ensure GDPR requirements are met when data Is shared.
- 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)

13. 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).

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.

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).

* 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).

14. Personal devices and bring your own device (BYOD) policy

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~~Digital~~

Form

~~images and video~~ section and **Error! Reference source not found.**~~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.

15. 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~~Digital images and video~~ section and **Error! Reference source not found.**~~Data protection and data security~~ section of this document. Child/staff data should never be downloaded onto a private phone.

Form

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 other than via Guest WiFi

16. Visits / events away from school

For school visits /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.

17. Remote Learning

In response to School Closures and the Pandemic SVMAT Schools have adopted various Remote Learning methods to deliver learning via 'live' lessons, recorded lessons or other platforms that support the teaching and learning for pupils.

These arrangements require staff, pupils and parents to follow clear procedures and practices that can be found on the School website under 'remote learning' policy.

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.

Linked Policies

Child Protection Policy

Data Protection Policy

Staff Code of Conduct

Remote Learning Policy (School specific)

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:**