360safe
the online safety self-review tool

Mid-Trent
Multi Academy Trust

Online Safety Policies
September 2023

St Andrew's CE Primary School	Colwich CE Primary School	St Peter's CE Primary School	Flourish Early Education

Document Control Information

Document ID	MTMAT040
Document title	Online Safety Policy
Version	1.1
Status	APPROVED
Author	Paul Hayward (Headteacher on behalf of MT MAT)
Publication date	21.09.2023
Review Cycle	Annually
Next Review Due	September 2024

Version History				
Version	**Date**	**Detail**	**Author**	**Key Changes**
1.0	31.10.2022	Initial	P. Hayward	New policy
1.1	21.09.2023	Review	C. Pilkington	Changes made to include information from KCSiE 2023; Filtering and Monitoring Policy reviewed. Policy reorganised to aid reading for understanding.

Approval History			
Version	**Approver**	**Date**	**Included in the minutes of**
1.0	MAT Board		MAT Board – Spring 1
1.1	CEO	21.09.2023	Leadership Forum Minutes 21.09.2023

Mid-Trent
Multi Academy Trust

Online Safety Policy

1. Introduction

The DfE guidance “Keeping Children Safe in Education” states:

> “Online safety and the school or college’s approach to it should be reflected in the child protection policy”

The school Online Safety Policy:

- Sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- Allocates responsibilities for the delivery of the policy
- Is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- Establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- Describes how the school will help prepare learners to be safe and responsible users of online technologies
- Establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- Is supplemented by a series of related acceptable use agreements
- Is made available to staff at induction and through normal communication channels (to be described)
- Is published on the school website.

2. Scope of the Policy

This Online Safety Policy outlines the commitment of the Mid-Trent MAT to safeguard members of our school communities whilst online in accordance with statutory guidance and best practice.

This policy applies to all members of the Mid-Trent MAT community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of Trust digital technology systems, both in and out of Trust schools.

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

3. Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the Trust.

Board of Directors

The DfE guidance "Keeping Children Safe in Education" states:

> *"Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare …. this includes … online safety"*
>
> *"Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)"*

Directors at Mid-Trent MAT are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the directors receiving regular information about online safety incidents and monitoring reports. A member of the Board has taken on the role of Online Safety Director (This is combined with that of the Child Protection/Safeguarding Governor).

Mid-Trent MAT Director responsible for Online Safety:	Mrs Kerry Reynolds

The role of the Online Safety Director will include:

- Regular meetings with the Designated Safeguarding Lead / Online Safety Lead
- Regularly receiving (collated and anonymised) reports of online safety incidents
- Checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards
- Reporting to relevant governors group/meeting
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards

The Board of Directors and each school's Local Academy Committee will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, they maintain responsibility as Designated Safeguarding Leads for responding to and monitoring Online Safety incidents, though the day to day responsibility for monitoring, educating and promoting online safety may be delegated to the Online Safety Lead.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Headteacher and each school's Local Academy Committee (LAC) will receive regular monitoring reports from the Online Safety Lead.

Designated Safeguarding Lead

Keeping Children Safe in Education states that:

"The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder's job description."

They (the DSL) "are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college"

They (the DSL) "can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online"

The Designated Safeguarding Leads in our Trust Schools are:

Colwich CE Primary School	St Andrew's CE Primary School	St Peter's CE Primary School
Mrs Alison De Ste Croix	Mr Paul Hayward	Mrs Charlotte Pilkington

While the responsibility for online safety is held by the DSL and cannot be delegated, in some of our Trust Schools an Online Safety Lead is appointed to work in support of the DSL in carrying out these responsibilities.

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings/groups
- report regularly to headteacher/senior leadership team
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

Online Safety Lead

The Online Safety Leads in Trust Schools are:

Colwich CE Primary School	St Andrew's CE Primary School	St Peter's CE Primary School
Mrs Alison De Ste Croix	Mr Paul Hayward	Mr Tom Gray

The Online Safety Lead will:

- Work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL), (where these roles are not combined)
- Receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- Have a leading role in establishing and reviewing the school online safety policies
- Promote an awareness of and commitment to online safety education
- Raising awareness of online safety issues across the school and beyond
- Liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- Provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- Liaise with technical staff, pastoral staff and support staff (as relevant)
- Receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:

  content
  contact
  conduct
  commerce

Network Manager/ IT Provider

The DfE Filtering and Monitoring Standards says:

> *"Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider."*
>
> *"Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support."*
>
> *"The IT service provider should have technical responsibility for:*
>
> - *maintaining filtering and monitoring systems*
> - *providing filtering and monitoring reports*
> - *completing actions following concerns or checks to systems"*
>
> *"The IT service provider should work with the senior leadership team and DSL to:*
>
> - *procure systems*
> - *identify risk*
> - *carry out reviews*
> - *carry out checks"*
>
> "We are aware that there may not be full-time staff for each of these roles and responsibility may lie as part of a wider role within the school, college, or trust. However, it must be clear who is responsible, and it must be possible to make prompt changes to your provision."

School's within the Mid-Trent MAT contract the support of IT Providers and Network Managers through a service level agreement with Core Education. The person with responsibility for technical support and ensuring the effective management of school networks in each school are:

Colwich CE Primary School	St Andrew's CE Primary School	St Peter's CE Primary School
Theo Pavlou Core Education	Theo Pavlou Core Education	Theo Pavlou Core Education

Those with technical responsibilities are responsible for ensuring that:

- They are aware of and follow the Trust's Online Safety Policies (inc. Technical Security Policy) to carry out their work effectively in line with these policies.
- The school technical infrastructure is secure and is not open to misuse or malicious attack
- The school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority / MAT or other relevant body
- There is clear, safe, and managed control of user access to networks and devices
- They keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- The use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to (insert relevant person) for investigation and action
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person (see appendix 'Technical Security Policy template' for good practice).

- Monitoring systems are implemented and regularly updated as agreed in school policies.

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current Trust online safety policy and practices
- They have read, understood and signed the staff acceptable use agreement (AUA)
- They report any suspected misuse or problem to the Headteachers or Online Safety Leads for investigation, action and/or sanction as appropriate
- All digital communications with pupils and parents/carers should be on a professional level and only carried out using official school systems
- Online safety issues are explored and embedded in all aspects of the curriculum and wider school activities
- Pupils understand and follow this Online Safety Policy and appropriate acceptable use agreements
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (particularly for upper KS2)
- They monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Pupils:

- Are responsible for using the Trust digital technology systems in accordance with the pupil acceptable use agreements
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (upper KS2 particularly)
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Are expected to know and understand the Trusts expectations for the use of mobile devices in school. They should also know and understand policies on the taking/use of images and on online-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the Trust's online safety policy covers their actions out of school, if related to their membership of the school.

Parents/Carers:

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The Trust will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support Trust schools in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the school website/communication system and on-line pupil records
- their children's personal devices in Trust schools

Community Users:

Community Users who access Trust systems or programmes as part of the wider Trust schools provision will be expected to sign the Trust's Community User AUA before being provided with access to Trust school systems.

4. Acceptable Use

The Mid-Trent MAT has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

Acceptable use agreements

Our MAT Acceptable Use Agreements outline the Trust’s expectations on the responsible use of technology by its users. The agreements (see appendices) are regularly promoted, understood and followed by all users within our Trust school communities.

These agreements are communicated and regularly re-enforced through:

- Annual consents
- Staff induction and handbook
- Splash screens
- Posters/notices around where technology is used
- Communication with parents/carers
- Built into education sessions
- School website

4a. Acceptable Use – User Activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 N.B. Schools/academies should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					🟥
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					🟥
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					🟥

that contain or relate to:	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					🟥
	Pornography				🟨	
	Promotion of any kind of discrimination				🟨	
	threatening behaviour, including promotion of physical violence or mental harm				🟨	
	Promotion of extremism or terrorism				🟨	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school/Trust or brings the school/Trust into disrepute				🟨	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					🟨	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					🟨	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					🟨	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)					🟨	
Using school systems to run a private business					🟨	
Infringing copyright					🟨	
On-line gaming (educational eg TT Rockstars)		🟩				
On-line gaming (non-educational)					🟨	
On-line gambling					🟨	
On-line shopping/commerce (eg Ordering from Amazon using MAT Business card)				🟨		
File sharing		🟩				
Use of social media (School Facebook, Class Dojo)				🟨		
Use of messaging apps				🟨		
Use of video broadcasting e.g. Youtube				🟨		

4b. Acceptable Use – Communication Technologies

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Personal mobile phones may be brought to the school		🟧				🟧		
Use of mobile personal phones in lessons				🟥				🟥
Use of school phones in lessons			🟧				🟧	
Use of mobile personal phones in social time	🟩							🟥 *
Taking photos on personal mobile phones/cameras				🟥				🟥
Taking photos on school mobile phones/cameras			🟧				🟧	
Use of other personal mobile devices e.g. tablets, gaming devices		🟧						🟥
Use of personal email addresses in school, or on school network		🟧						🟥
Use of school email for personal emails				🟥				🟥
Use of personal messaging apps		🟧						🟥
Use of personal social media		🟧						🟥
Use of personal blogs		🟧						🟥

** There may be occasions, not within the school day, when children of staff members may be permitted to use their personal devices under the supervision of their parent. Permission should be sought by the staff member from the Headteacher in this instance and not assumed.*

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

- The official school email service is regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the Designated Safeguarding Lead, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email, Class Dojo, MS Teams, school website) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

- Personal information should not be posted on school websites and only official email addresses should be used to identify members of staff.

5. Reporting and Responding to Incidents of Misuse

Reporting to an Online Safety Incident

Our MAT schools will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. In our schools:

- There are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- All members of the school community are aware of the need to report online safety issues/incidents
- Reports are dealt with as soon as is practically possible once they are received
- The Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- If there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), the incident will be escalated through the agreed school safeguarding procedures.
- Any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of the Local Academy Committee and the CEO.

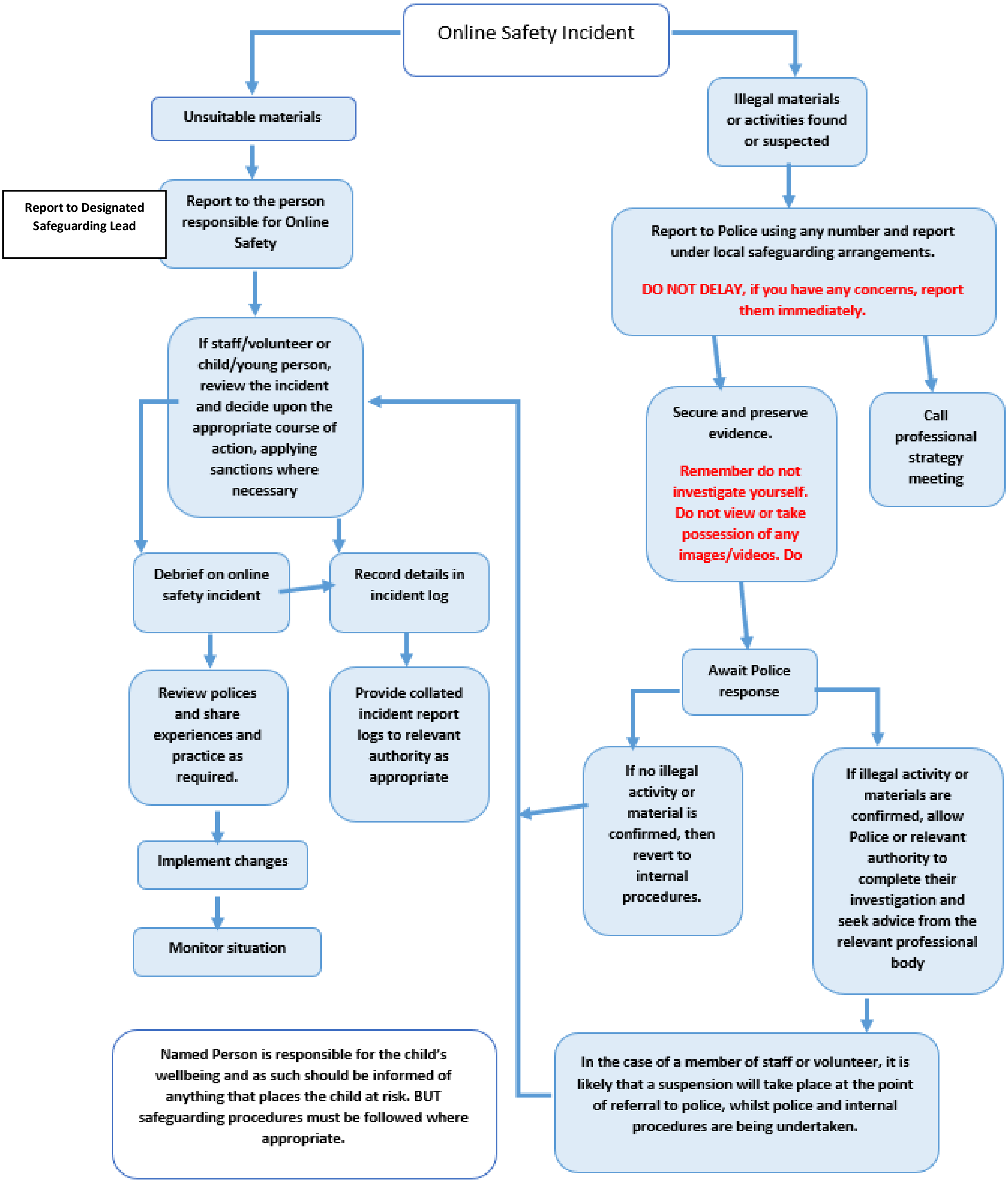
Responding to an Online Safety Incident

Where there is no suspected illegal activity, devices may be checked using the following procedure:

- One or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
- Ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:

- internal response or discipline procedures
- involvement by local authority / MAT (as relevant)
- police involvement and/or action

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.


Online Safety Incident
Unsuitable materials
Report to Designated Safeguarding Lead
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Actions and Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Pupil Incidents	Refer to class teacher/tutor	Refer to Headteacher	Refer to Police	Refer to technical support staff for	Inform parents/carers	Removal of network/internet	Warning	Further sanction e.g.
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X		X			
Unauthorised use of non-educational sites during lessons	X	X			X		X	
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device		X			X		X	X
Unauthorised/inappropriate use of social media/ messaging apps/personal email		X			X		X	
Unauthorised downloading or uploading of files		X			X		X	
Allowing others to access school network by sharing username and passwords		X			X	X	X	
Attempting to access or accessing the school network, using another pupil's account	X	X			X		X	
Attempting to access or accessing the school network, using the account of a member of staff		X			X			X
Corrupting or destroying the data of other users		X			X			X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X			X	X	X	
Continued infringements of the above, following previous warnings or sanctions		X			X			X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X			X		X	
Using proxy sites or other means to subvert the school's filtering system		X			X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident		X		X	X			
Deliberately accessing or trying to access offensive or pornographic material		X		X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X			X			

Staff Incidents	Refer HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).	X	X	x	X		X
Inappropriate personal use of the internet/social media/personal email	X		X	X		X
Unauthorised downloading or uploading of files	X			X		X
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X		X	X		X
Careless use of personal data e.g. holding or transferring data in an insecure manner	X			X		X
Deliberate actions to breach data protection or network security rules	X				X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X				X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X					X
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils	X			X	X	X
Actions which could compromise the staff member's professional standing	X			X		
Actions which could bring the school or Trust into disrepute or breach the integrity of the ethos of the school or Trust	X			X		X
Using proxy sites or other means to subvert the school's filtering system	X			X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X			X		X
Deliberately accessing or trying to access offensive or pornographic material	X				X	X
Breaching copyright or licensing regulations				X		
Continued infringements of the above, following previous warnings or sanctions					X	X

Recording an Online Safety Incident

All Online Safety incidents should be recorded logged on a PINK Online Safety Concern Report which includes details of the incident, those involves, the investigation, the outcome and the actions taken.

Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant).

Learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:

- staff, through regular briefings
- learners, through assemblies/lessons
- parents/carers, through newsletters, school social media, website
- Local Academy Committees, through regular safeguarding updates
- Local authority/external agencies, as relevant

6. Online Safety Education Programme

Education – Pupils

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

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum is provided as part of PSHE, complimented through computing and addressed across the curriculum to ensure that key messages are regularly revisited.
- Key online safety messages are reinforced as part of a planned programme of pastoral activities and informally through responses to developing risks (eg. new games/ apps) and incidents as they arise.
- Pupils are taught to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils are helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff will be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff temporarily remove specific sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need and on such occasions, free-searching is not permitted.

Education – Parents/Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, web site, Learning Platform
- Parents/carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications e.g. swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers

Education & Training – Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the Trust's online safety policy and acceptable use agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff in staff meetings.
- The Online Safety Lead will provide advice, guidance and training to individuals as required.

Training – LAC Members and MAT Directors

School LAC Members and MAT Directors should take part in online safety training sessions, with particular importance for those who are members of any group involved in online safety, health and safety and/or safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority, MAT, National Governors Association or other relevant organisation.
- Participation in school training, information sessions for staff or parents.

Monitoring and Review of this Policy

Monitoring

Trust schools will regularly monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) and filtering logs
- Internal monitoring data for network activity
- Surveys of pupils, parents/carers and staff.

Review

This policy was originally published in October 2022; reviewed in September 2023 and is due for review again in September 2024.

This policy is approved by the CEO on behalf of the Mid-Trent MAT Board of Directors on an **annual** basis.

Technical Security Information

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The Trust is responsible for ensuring that the school network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security is the responsibility of the school's IT provider (Core Education) under the supervision of the Headteacher of each Trust school.

Technical Security

The Trust is responsible for ensuring that their network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school/academy systems and data
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff
- All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the MAT CEO and will be reviewed, at least annually, by the Headteacher's Leadership Forum.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Office administrators in each school are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Procedures for managing school-owned and personal mobile devices are in place and regularly reviewed.

- Headteacher's regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement. School's within the Mid-Trent MAT use SENSO to monitor activity on the school's network and managed devices.
- An appropriate system is in place (direct report to Headteacher/ Online Safety Lead) for users to report any actual or potential technical incident.
- An agreed policy is in place for the provision of temporary access of "guests", (e.g. trainee teachers, supply teachers, visitors) onto the school system. Regular supply teachers, trainee teachers and visitors will be issued with a unique username and password. Infrequent supply staff will use guest log ins which will be provided and recorded by the school office.
- Only network administrators are permitted to download executable files and the install programmes on school devices.
- An agreed policy (see Mobile devices section above) is in place regarding the extent of personal use that users (staff/learners/community users) and their family members are allowed on school/academy devices that may be used out of school.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices (see data protection policy for more information). Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.

Mid-Trent
Multi Academy Trust

Password Security Policy

A safe and secure username/password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and learning platform).

Policy Statements:

These statements apply to all users:

- All school networks and systems will be protected by secure passwords.
- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the MAT CEO and will be reviewed, at least annually, by the MAT Leadership Forum.
- All users (adults and students/pupils) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords must not be shared with anyone.
- All users will be provided with a username and password by the school's Online Safety Lead/ Network Manager who will keep an up to date record of users and their usernames.

Password Requirements:

- Passwords should be personal and not easily guessed by others. Users are aware that good passwords are over 12 characters in length and should include a combination of unconnected words.
- Each user has a different password for their account (no generic pupil passwords are in use). This ensures that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school.
- Passwords must not include names or any other personal information about the user that might be known by others.
- Passwords must be changed on first login to the system.
- Staff passwords expire every 3 months and a new password is required.

Pupil Passwords:

- All pupils have a unique username and password meaning that all accounts can be accurately monitored through the school's monitoring system.
- Class teachers may keep paper/ electronic records of pupil passwords to support learners in accessing their pupil accounts. Lists of pupil passwords must be kept securely.
- Pupil passwords do not expire but users will be required to change their password if it is compromised.
- Pupils will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

Technical Staff Passwords:

- Each administrator should have an individual administrator account, as well as their own user account with access levels set at an appropriate level. Where available, two factor authentication is in place for administrator accounts.
- An administrator account password for the school systems should also be kept in a secure place e.g. school safe. This account and password should only be used to recover or revoke access. Other administrator accounts should not have the ability to delete this account.

- Passwords for new technical/ administrative users, and replacement passwords for existing users will be allocated by the Headteacher (for technical and administrator permissions) or the Online Safety Lead. Passwords set or re-set in this way are temporary and users will be prompted to change their passwords at the first log-in.
- Requests for password changes should be authenticated by the Headteacher or Online Safety Lead in school to ensure that the new password can only be passed to the genuine user.
- 'Guest' log ins are only used in very rare circumstances (eg. new/ unfamiliar supply cover), these are allocated by the office administrator and the password changed after each use.
- Staff and Pupil accounts "locked out" following six successive incorrect log-on attempts.
- Passwords shall not be displayed on screen, and shall be securely hashed when stored (use of one-way encryption).

Training/Awareness:

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's online safety policy and password security policy
- through the acceptable use agreement

Students/pupils will be made aware of the school's/college's password policy:

- annually in lessons when reviewing the pupil acceptable use agreement and in specific online safety lessons
- through the introduction and regular review of the pupil acceptable use agreement

Mid-Trent
Multi Academy Trust

Filtering and Monitoring Policy

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. This Filtering and Monitoring policy is reviewed annually to support Trust schools in managing the associated risks and to provide appropriate preventative measures, in line with the DfE's Filtering and Monitoring Standards.

Filtering

- Individual Trust schools manage access to content across its systems for all users and on all devices using the schools internet provision.
- The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- illegal content (e.g., child sexual abuse images) is filtered by RM Safety Net (the Trust's broadband and filtering provider) by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated within the RM SafetyNet system.
- Trust schools can, with a clear educational reason, request for changes to the standard filtering through contacting RM SafetyNet.
- Requests to access specific websites which are normally blocked by filtering services, must be approved by the Headteacher, who will determine which users are able to access the website requested. This is usually limited to staff only, with standard filtering in place for pupils.
- Filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- Trust school's provide differentiated user-level filtering (staff/pupils).
- The Trust has a mobile technologies policy and where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
- Access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.
- Headteachers regularly test their filtering for protection against illegal materials using SWGfL Test Filtering
- If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- Monitoring reports (provided by SENSO) are regularly received, reviewed and acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.

- There are effective protocols in place to report abuse/misuse of the school's filtering policies.
- There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
- Trust schools follow the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. These include:
  - physical monitoring (adult supervision in the classroom)
  - internet use is logged, regularly monitored and reviewed
  - filtering logs are regularly analysed and breaches are reported to senior leaders
  - pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
- Headteachers regularly monitor and record the activity of users on the school technical systems through regular access and reporting within SENSO software.
- School owned mobile devices and IPADs are monitored through ???.
- Monitoring reports are reviewed monthly by the CEO as a quality assurance check for Headteachers.
- Monitoring reports are reviewed annually by each school's Local Academy Committee (may be delegated to the LAC member with responsibility for Online Safety).

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the Headteacher. They will manage the school filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- be logged in change control logs
- be reported to and authorised by a second responsible person prior to changes being made (Online Safety Lead/ Deputy Designated Safeguarding Lead)
- be reported to the LAC Member/ Director for Online Safety annually in the form of an audit of the change control logs

All users have a responsibility to report immediately to the Online Safety Lead any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials, this is made clear within both the staff and pupil acceptable use agreements.

Education/Training/Awareness

Pupils will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- the acceptable use agreement
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the acceptable use agreement and through online safety awareness sessions/newsletter etc.

Changes to the Filtering System

- Any staff member may request a change to the school's filtering system. This should be requested in writing (usually email) with a clear rationale as to why a bypass of the school filtering is required for educational purposes.
- Requests will be reviewed by the Headteacher and assessed on the grounds of educational benefit vs risk of bypassing the filtering system.
- If a request is approved by the Headteacher, it will be forwarded to the Online Safety Lead/ Deputy Designated Safeguarding Lead for review and agreement.
- If agreed, the request will be made to the school's Network Manager and actioned.
- All requests and outcomes will be logged within the school's reporting log and shared with the Online Safety Lead and the LAC Member/ Director for online safety as part of regular reviews.
- Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the school's online safety lead who will decide whether to make school level changes (as above).

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the school online safety policy and the acceptable use agreement. Formal monitoring will take place weekly through the school's monitoring system (SENSO) which is completed by the Headteacher and also informally, within lessons by class teachers who will have an overview of pupils internet use in school.

Audit/Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- The second responsible person (Designated Safeguarding Lead).
- Online Safety Lead
- Online Safety LAC Member/ Director of Online Safety
- External Filtering provider/Local Authority/Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

Mobile Technologies Policy

Mobile Technologies Policy

Mobile technology devices may be school owned or personally owned and might include: smartphones, tablets, notebook/laptops or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile devices in a school context is educational. This online safety policy is consistent with and inter-related to other relevant school polices including but not limited to the safeguarding policy, behaviour policy, bullying policy, acceptable use agreements, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

- The school acceptable use agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies
- Trust schools allow:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	Yes	Yes	Yes	Yes	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only	-	-	-	No	Yes	No
Network access	Yes	Yes	Yes	No	No	No

Pupil Owned Mobile Devices:

Pupils across the MAT are permitted to bring mobile phones into school for the purpose of ensuring pupil safety walking to and from school without adult supervision (this is usually in Year 5/ Year 6 only). Personal mobile devices are switched off and secured away from pupils on entry into school each day and re-issued to them at the end of the day.

Pupils are not permitted to bring any other mobile devices (eg. games consoles/ hand-held devices/ smart watches – with capacity to receive/ send messages and or record) into school without the express permission of the headteacher.

Staff Owned Mobile Devices:

The MAT Code of Conduct (section 2.8) states that:

Staff are not allowed to make and receive calls, or send texts, except at lunchtime or during breaks when away from pupils. Staff are permitted to use the school’s wifi (if necessary as a result of poor signal) to access the internet on personal devices, however they must ensure that they comply with the Trust’s Online Safety Policy and the school’s acceptable use agreement at all times, even when using their personal device.

School’s provide staff with mobile devices (IPads/ Mobile phones) to support them in their work, therefore staff and/or volunteers are not permitted to use personal mobile devices to take photographs/videos of children and thus images of children and/or children’s personal data should not be stored on these devices.

Mobile Phones in Early Years

In line with our MAT Early Years policy, all Early Years settings within the MAT have a no mobile phone policy and parents, staff, volunteers and visitors are not permitted to use their personal mobile phones within the setting or directly outside the setting to ensure the safety of all children. Signs are in place on entry into each setting to alert parents, visitors and staff of this. In our Early Years settings, staff mobile phones are placed in a sealed box and stored in the staff cupboard on entry to the setting each day.

School’s provide staff with mobile devices (IPads/ Mobile phones) to support them in their work, therefore staff and/or volunteers are not permitted to use personal mobile devices to take photographs/videos of children and thus images of children and/or children’s personal data should not be stored on these devices.

School-Owned Mobile Devices:

School-owned mobile devices are subject to the general staff acceptable use policy and must be used in accordance with this. In addition, the school’s Mobile Devices Acceptable Use Policy outlines specific dos and donts when using school-owned mobile devices such as IPads and Mobile phones. As per these agreements, staff members are not permitted to use school owned devices for personal use whether at school or at home, this includes personal email, accessing social media accounts and online shopping.

Mid-Trent
Multi Academy Trust

Use of digital and video images Policy

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website, social media or in local/ national press. This is obtained through annual consent collection each September.
- In accordance with guidance from the Information Commissioner’s Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone’s privacy and in some cases to protect children at risk of harm, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images. This expectation is clearly communicated to parents/carers at the start of all in-school events.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow Trust policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school/Trust into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils’ full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil’s work can only be published with the permission of the pupil and parents or carers.

Data Protection Policy

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

Trust schools must ensure that:

- They have a Data Protection Policy.
- They implement the data protection principles and are able to demonstrate that they do so through use of policies, notices and records.
- They have paid the appropriate fee to the Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- They have appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
- They have an 'information asset register' in place and know exactly what personal data is held, where this data is held, why and which members of staff have responsibility for managing it.
- The information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded.
- They will hold only the minimum personal data necessary to enable them to perform their function and will not hold it for longer than necessary for the purposes it was collected for. Personal data held must be accurate and up to date where this is necessary for the purpose it is processed for.
- Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals.
- The Trust provides staff, parents, volunteers, teenagers and older children with information about how Trust schools looks after their data and what their rights are in a clear Privacy Notice, which is published annually on each school's website.
- Procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- Data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier.
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners.
- They have undertaken appropriate due diligence and have required data processing clauses in contracts in place with any data processors where personal data is processed.
- They understand how to share data lawfully and safely with other relevant data controllers.
- They report any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. They also report relevant breaches to the individuals affected as required by law. In order to do this, the Trust has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- They have a Freedom of Information Publication Scheme which sets out how it will deal with FOI requests.
- All staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

- data must be encrypted and password protected.

- device must be password protected.
- device must be protected by up to date virus and malware checking software.
- data must be securely deleted from the device, in line with Trust policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- understand where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- will not transfer any school personal data to personal devices except as in line with school policy
- access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.

Social Media - Protecting Professional Identity

All schools and MATs have a duty of care to provide a safe learning environment for pupils and staff. Schools and MATs could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or MAT liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

Trust schools provide the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or MAT
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school/academy social media accounts are established there should be:

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

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the Trust or a Trust school or impacts on the Trust, it must be made clear that the member of staff is not communicating on behalf of the Trust with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon a Trust school or the Trust itself are outside the scope of this policy
- The Trust permits reasonable and appropriate access to private social media sites outside of working hours, however where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.
- The school's use of social media for professional purposes will be checked regularly by the headteacher to ensure compliance with the school policies.

Online Safety Policy Appendices

Pupil Acceptable Use Agreement (Y5/Y6)

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

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online-bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Agreement

This acceptable use agreement will be discussed with pupils in class during the first weeks of the Autumn term, this will include time for questions and to ensure pupil understanding of its content. Pupils will understand that their access to school systems is dependent upon them upholding this agreement at all times.

Simplified Pupil Acceptable Use Agreement (R-Y4)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet

Agreement

This acceptable use agreement will be discussed with pupils in class during the first weeks of the Autumn term, this will include time for questions and to ensure pupil understanding of its content. All pupils will click to accept this agreement when the log into school computers/ devices. Pupils will understand that their access to school systems is dependent upon them upholding this agreement at all times.

Parent Acceptable Use Agreement

2023-2024

Mid-Trent
Multi Academy Trust

Parent Agreement

Introduction
New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The Trust and its schools will ensure that learners will have good access to ICT to enhance their learning and will, in return, expect the learners to agree to be responsible users. A copy of the pupil acceptable use agreement is provided to parents/carers annually so that you are aware of the school's expectations for pupils when accessing or using school systems and networks.

Parent/Carer Agreement:
As a parent/carer:

- I know and understand that my child has been informed of the pupil acceptable use agreement and will receive regular online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- I understand that my child's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.
- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Agreement

Parents/carers are asked to consent to this agreement when their child starts school and the contents is re-shared annually to ensure continual understanding. Parents/carers are made aware that they have the right to withdraw their agreement at any time in writing through the school office.

Specific Consent for the use of Photographs/ Video

2023-2024

As part of the school's compliance with General Data Protection Regulations, your consent is requested for the use of your child's image and name for the following purposes. We collect this consent information once, when your child begins school, however you are welcome to withdraw your consent at any time through requesting a new photograph permissions form.

I give my consent for the following information relating to my child to be used in school:	
Individual Portrait Photographs (eg. from school photographs) to be stored on the Office secured hard drive (these are used for pupils' internal records).	Yes/ No
Class Photographs which will be shared with all parents of children in the class.	Yes/ No
Photographs of learning to be stored on the school's secure server (these are used to evidence learning and to celebrate success in school displays).	Yes/ No
Photographs of my child to be posted on the school website/ digital prospectus.	Yes/ No
Videos of my child to be posted on the school website/ digital prospectus.	Yes/ No
My child's name to be used on the school website.	Yes/ No
Photographs of my child to be used on the school newsletter.	Yes/ No
My child's first name to be used in the school newsletter.	Yes/ No
My child's image to be used in promotional materials used within school (e.g. printed posters on the internal walls).	Yes/ No
My child's image to be used in promotional materials to be distributed beyond the immediate school community (eg. advertisements, MAT website).	Yes/ No
My child's image to be used in the press (online and in paper format)	Yes/ No
My child's name to be used in the press (online and in paper format)	Yes/ No
Signed (Parent/ Guardian): **Date:**	

Specific Consent for the use of Cloud Based Systems 2023-2024

The school uses Microsoft Office 365 for pupils and staff. This permission form describes the tools and pupil responsibilities for using these services.

The following services are available to each pupil as part of the school's online presence in Office 365:

- MS Word
- MS Powerpoint
- MS Excel
- MS OneDrive
- MS Sharepoint
- MS Teams (Video Conferencing Software)

Using MS Office 365 will enable your child to collaboratively create, edit and share files and websites for school related projects and communicate via MS Teams with other pupils and members of staff. These services are entirely online and available 24/7 from any internet-connected computer.

Following an assessment of the risk of using cloud based services, such as MS Office 365, the school believes that access to these tools significantly benefits pupils' quality of education, through allowing them to engage in learning during school closure periods (eg. snow days) and also through accessing professional applications to complete and submit home-learning safely. tools significantly adds to your child's educational experience.

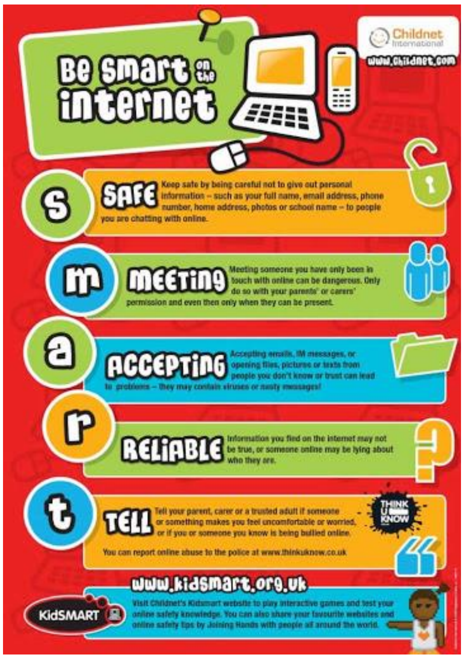
An acceptable use agreement is in place for home learning/ remote learning which covers the expectations for pupil's online behaviour when accessing MS Office 365 services outside of school (see attached).

Mid-Trent
Multi Academy Trust

Pupil Acceptable Use Policy for Home Learning and Remote Education

When using Office 365 applications:

1. We will learn using the applications in Office 365, for example: SharePoint, OneDrive and TEAMs
2. We must only use our school account to log on and complete our home learning.
3. We can contact our class teachers between 8.30am and 4.30pm, but they might not be able to answer us straight away.
4. We will attend live lessons which are on our timetable and let school know if we are not able to join for any reason.
5. We will dress appropriately for live lessons (smart/casual) and blur our backgrounds to avoid unnecessary distractions.
6. We will catch-up with any live lessons we have missed using the videos which will be made available after the lesson.
7. We will complete our learning in a shared space where there are grown-ups around to help me if I need it.
8. We will complete the work on our timetable each day and share it with our class teachers so that they can give us some feedback on how to keep getting better.
9. We will tell our teachers if we are finding learning too difficult/ too easy so that they can adapt it for us.
10. We will remember that all our communications using our school accounts are monitored, this includes email and chat, so we will use the 'Nanna Check' before sending any messages. All communications will be professional in tone and we will always use the correct punctuation and grammar.



S SAFE Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.

M MEETING Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

A ACCEPTING Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

R RELIABLE Information you find on the internet may not be true, or someone online may be lying about who they are.

T TELL Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

You can report online abuse to the police at www.thinkuknow.co.uk

www.kidsmart.org.uk

Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.

11. We will remember our online safety rules when we are working and always tell a grown up if we see or hear anything that worries us.

12. We will only log into Office 365 using our own username and password and never share our personal information with other people.

- We are gentle
- We are kind and helpful
- We listen
- We are honest
- We work hard
- We look after our property

13. We will behave online like we do in the classroom and remember that our Golden Rules still apply here.

Staff (and Volunteer) Acceptable Use Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.

- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my own mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use (see staff code of conduct). I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems (this includes school-owned mobile devices such as phones and laptops).
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school/academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the MAT Data Protection Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/directors and/or the Local Authority and in the event of illegal activities the involvement of the police.

Agreement

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name:	
Signed:	
Date:	

This agreement may be accepted in writing or via an online form, with a linked school email address.

School Mobile Devices Acceptable Use Agreement

The MAT staff (and volunteer) acceptable use policy applies to the use of school-owned mobile phones in its entirety. In particular school-mobile phone users should note that:

- School mobile phones are to be used in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.
- The school will monitor the use of school mobile phones, inc. app useage, location and communications.
- They must not transfer photographs or data from these devices (digital or paper) outside of school owned storage (OneDrive/Sharepoint) or communication systems (school email/ classdojo).
- They must use school mobile phones responsibly and ensure all use is primarily intended for educational purposes. School mobile phones must not be used for personal or recreational use (Personal emails, Spotify, YouTube, Facebook etc.)
- School mobile phone passwords must remain unchanged to allow for appropriate monitoring and upgrades.
- School mobile phones should not be taken off school premises without the express permission of the Headteacher/ Deputy Headteacher. Devices must be signed out at the office and signed back in.
- Staff must report immediately any illegal, inappropriate or harmful material or incident, they become aware of, to the Headteacher.
- Staff must communicate (via dojo or email) with parents/carers, staff and other professionals in the same professional manner as would be expected when conversing on a PC or in person.
- Staff use school phones to capture images and videos of children with a clear and intended educational purpose (capturing learning/ evidencing learning/ wow moments to share with parents/carers) and end destination (Onedrive/Sharepoint/ClassDojo/Teams/Pupil’s Online Portfolios eg. 2simple/ClassDojo).
- Staff ensure that images and videos of children are shared in line with the consent of parents/carers.
- Staff regularly review and delete photographs and images of children from school-mobile phones (once uploaded/shared).
- Staff will not add/ remove apps from school-owned mobile phones without permission from the Headteacher/ IT provider.
- Staff will not switch off location notifications on school-owned mobile phones.
- Staff will not engage in any on-line activity that may compromise their professional responsibility.
- Staff will endeavour to ensure that school-owned mobile devices are looked after when in their possession, ensuring they remain in a case with a screen protector in place. Staff will report any damage or faults involving equipment or software, however this may have happened to the Headteacher as soon as practicable.

I have read and understand the above and agree to use school-owned mobile devices (inc. school-owned mobile phones) within these guidelines. I understand that failure to comply with the guidelines contained within this acceptable use policy may result in disciplinary action in line with the MAT Staff Discipline Policy.

Staff/Volunteer Name:	
Signed:	
Date:	

Online Safety Incident Reporting Log

Schools may choose to record online safety incidents using this reporting log in paper form or electronically.

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Supporting Resources

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/

South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/

Childnet – http://www.childnet-int.org/

Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline

Revenge Porn Helpline - https://revengepornhelpline.org.uk/

Internet Watch Foundation - https://www.iwf.org.uk/

Report Harmful Content - https://reportharmfulcontent.com/

CEOP

CEOP - http://ceop.police.uk/

ThinkUKnow - https://www.thinkuknow.co.uk/

Others

LGfL – Online Safety Resources

Kent – Online Safety Resources page

INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/

UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Netsmartz - http://www.netsmartz.org/

Tools for Schools

Online Safety BOOST – https://boost.swgfl.org.uk/

360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/

360Data – online data protection self-review tool: www.360data.org.uk

SWGfL Test filtering - http://testfiltering.com/

UKCIS Digital Resilience Framework - https://www.gov.uk/government/publications/digital-resilience-framework

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/

SELMA – Hacking Hate - https://selma.swgfl.co.uk

Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/

Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388

DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Childnet – Cyberbullying guidance and practical PSHE toolkit: http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit

Childnet – Project deSHAME – Online Sexual Harrassment

UKSIC – Sexting Resources

Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

Ditch the Label – Online Bullying Charity

Diana Award – Anti-Bullying Campaign

Social Networking

Digizen – Social Networking

UKSIC - Safety Features on Social Networks

Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum

SWGfL Evolve - https://projectevolve.co.uk

UKCCIS – Education for a connected world framework

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Data Protection

360data - free questionnaire and data protection self review tool

ICO Guides for Education (wide range of sector specific guides)

DfE advice on Cloud software services and the Data Protection Act

IRMS - Records Management Toolkit for Schools

NHS - Caldicott Principles (information that must be released)

ICO Guidance on taking photos in schools

Dotkumo - Best practice guide to using photos

Professional Standards/Staff Training

DfE – Keeping Children Safe in Education

DfE - Safer Working Practice for Adults who Work with Children and Young People

Childnet – School Pack for Online Safety Awareness

UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support

UKSIC – Appropriate Filtering and Monitoring

SWGfL Safety & Security Resources

Somerset - Questions for Technical Support

NCA – Guide to the Computer Misuse Act

NEN – Advice and Guidance Notes

Working with parents and carers

Online Safety BOOST Presentations - parent's presentation

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

Get Safe Online - resources for parents

Teach Today - resources for parents workshops/education

Internet Matters

Prevent

Prevent Duty Guidance

Prevent for schools – teaching resources

NCA – Cyber Prevent

Childnet – Trust Me

Research
Ofcom –Media Literacy Research

Further links can be found at the end of the UKCIS Education for a Connected World Framework

Glossary of Terms

AUP/AUA	Acceptable Use Policy/Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MAT	Multi Academy Trust
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.
UKCIS	UK Council for Internet Safety
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol

A more comprehensive glossary can be found at the end of the UKCIS Education for a Connected World Framework

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in January 2020. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.