St Michael with St Thomas C of E Primary School

E-Safety Policy

Author: Principals/Directors
Owner: St Michael with St Thomas SLT
Date adopted: October 2020
Review: Summer 2023

We are a rights respecting school. All our policies and procedures are written and reviewed to ensure that children's rights, as detailed in the United Nations Convention on the Rights of the Child, are respected and promoted and this policy ensures:
Article 12*: All children have a right to be able to give their opinion when adults are making a decision that will affect them, and adults should take it seriously.*
Article 19: *All children should be protected from violence, abuse and neglect, and governments should protect them.*
Article 29: *Education should help children use and develop their talent and abilities. It should also help children learn to live peacefully, protect the environment and respect other people.*
Article 32: *Children should not be allowed to do work that is dangerous or might make them ill, or stop them going to school.*
Article 37: *No child should be punished in a way that humiliates or hurts them.*

For more information on the convention and the rights of each child visit: http://www.unicef.org.uk/

About the policy:

This policy applies to all members of The Three Saints Academy (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of the Three Saints Academy's ICT systems, both in and out of the Three Saints Academy. The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the Three Saints Academy's site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other E-safety incidents covered by this policy, which may take place outside of the Three Saints Academy, but is linked to membership of the Three Saints Academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the School's Behaviour and Relationships Policy.

St Michael with St Thomas Primary school will deal with such incidents within this policy and associated Safeguarding, Behaviour and Anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate E-safety behaviour that take place out of school.

Roles and Responsibilities:

The following section outlines the e-safety roles and responsibilities of individuals and groups within St Michael with St Thomas Primary school.

Board of Directors:

Directors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Directors receiving regular information.

The School Committee:

The School Committee will receive regular information, E-Safety incidents and monitoring reports.

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, this is delegated to the Designated Safeguarding Person (DSP) in respect of e-safety this is in liaison with the ICT Lead and IT Technician.
- The Headteacher and Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents "Responding to incidents of misuse".
- The Headteacher is responsible for ensuring that staff are sufficiently trained to carry out their e-safety roles.

- 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 e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

- The Senior Leadership Team and School Committee will receive regular monitoring reports from the Designated Safeguarding Person.

Designated Safeguarding Person (DSP):

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety documents with the computing Lead and IT Technician
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with the computing Lead and IT Technician (Agilisys)

- receives notification of e-safety incidents to inform future e-safety developments, this includes CPOMS e-safety logs from staff and from Need to Talk Button, a reporting app on our school website.
- SLT meet to discuss current issues and review incidents.
- reports regularly to the School Committee.
- Chairs E-safety group held annually with computing Lead and Agilisys IT Technician.
- Should be trained in E-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:
  - ✓ sharing of personal data
  - ✓ access to illegal / inappropriate materials
  - ✓ inappropriate on-line contact with adults / strangers
  - ✓ potential or actual incidents of grooming
  - ✓ cyber-bullying
  - ✓ risk of radicalisation

Computing Lead/Agilisys:

Agilisys and the computing Lead is responsible for ensuring:

- that the Academy's technical infrastructure is secure and is not open to misuse or malicious attack
- that St Michael with St Thomas primary school meets required e-safety technical requirements.
- that users may only access the networks and devices through passwords.
- Filtering is applied and updated on a regular basis to ensure:
  - ▪ No access to inappropriate internet content, malicious code and other threats;
  - ▪ provide controlled social media access;
  - ▪ Assist the Academy in meeting the Prevent Duty by keeping children safe from Terrorist and Extremist material
  - ▪ Detect expressions that are indicative of cyber bullying or self-destructive patterns.
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant

- that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation
- that monitoring software / systems are implemented and updated on a regular basis. School currently use Webscreen by Atomwide for filtering and Impero for monitoring within the classroom.

Teaching and Support Staff:

Are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current St Michael with St Thomas Primary school's E-Safety Policy and practices
- they have read, understood and signed the Acceptable User Policy (AUP) annually
- they report any suspected misuse or problem to the Headteacher / Designated Safeguarding Person
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- pupil's understand and follow the E-safety Policy and AUP and have their own child-friendly version which can be found within each year groups Purple Mash user agreement documents.
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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 students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Pupils:

- are responsible for using St Michael with St Thomas Primary school's digital technology systems in accordance with the AUP
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand the school's rules on the use of mobile devices and digital cameras. They should also know and understand rules on the taking / use of images and on cyber-bullying (see Anti-bullying policy and child friendly version).
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that St Michael with St Thomas Primary school's E-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. St Michael with St Thomas Primary school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, workshops and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support St Michael with St Thomas Primary school in promoting good e-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 website
- their children's personal devices within school (where this is allowed)

Visitors and Volunteers:

Visitors and Volunteers who access St Michael with St Thomas Primary school systems / website will be expected to agree to the AUP on sign in before being able to access the school's systems.

Policy Statements:

Education – Pupils:

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

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

- A planned e-safety curriculum should be provided as part of Computing / PHSE and other lessons and should be regularly revisited.
- The E-safety module on Purple Mash should be taught within Autumn 1 to ensure rules and acceptable behaviours are established before other ICT topics are perused.
- Key e-safety messages should be reinforced as part of the whole school curriculum.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be 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 should be supported in building resilience to grooming by providing a safe environment educating pupils to take a responsible approach to recognise and avoid e-safety risks in particular of giving personal information and posting images online.
- Pupils should be helped to understand the need for the AUP and encouraged to adopt safe and responsible use both within and outside St Michael with St Thomas Primary 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, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, monitoring is conducted by the use of Impero and access filtered using Webscreen by Atomwide. Staff should still

ensure that they are vigilant in monitoring the content of the websites the young people visit within lessons.

- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that Agilisys remove those sites from the filtered list for the period of study. Any request to do so, should be approved by the Headteacher.

Education – Parents / Carers:

Many parents and carers have only a limited understanding of e-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 on-line 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.

St Michael with St Thomas Primary school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Parents / Carers evenings / workshops
- High profile events such as Safer Internet Day
- Links to relevant web sites / publications via the school's website

Education & Training – Staff / Volunteers:

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

- Formal e-safety training is available to staff. This will be regularly updated and enforced.
- Designated Safeguarding Person holds a record of all staff safeguarding training including e-safety training.

All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand St Michael with St Thomas Primary school's E-safety Policy and AUP.

- This E-safety Policy and its updates will be presented to and discussed by staff in termly Department Meetings
- The Designated Safeguarding Person, Computing Lead and Agilisys will provide training to individuals as required.

Training – School Committee/ Directors:

Should take part in e-safety training / awareness sessions either by accessing Governor Training, school training or online training courses that are available.

Technical – infrastructure / equipment, filtering and monitoring:

St Michael with St Thomas Primary school has a managed computing service provided by Agilisys.

St Michael with St Thomas Primary school's technical systems are managed in ways that ensure that we meet recommended technical requirements

- There will be regular reviews and audits of the safety and security of the St Michael with St Thomas Primary school's technical systems
- All users will have clearly defined access rights to St Michael with St Thomas Primary school's technical systems and devices.
- All staff users are provided with a username and secure password. Users are responsible for the security of their username and password.
- All Pupils up to and including Year 5 log on to computers using a 'class' log on. Year 6 pupils are provided with their own username and password.
- The "administrator" passwords for each school within St Michael with St Thomas Primary school's computing system, used by Agilisys is available to the Headteacher and kept in a secure place (e.g. the school office safe)
- Agilisys and the school's Computing Lead 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.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by Agilisys using Webscreen by Atomwide Web Filtering software. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes (Headteacher's approval required)

- Internet filtering will ensure that children are safe from terrorist and extremist material when accessing the internet.
- St Michael with St Thomas Primary school has provided enhanced / differentiated user-level (i.e. pupils do not have access to streaming media whereas staff do.)
- Agilisys regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the AUP.
- The system in place for users to report any actual / potential technical incident / security breach is to contact the Computing Lead or Agilisys.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date Sophos virus software.
- The AUP is on sign in to St Michael with St Thomas Primary school's systems for the provision of temporary access of "visitors" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- The AUP is in place regarding the personal use that users are allowed on school devices that may be used out of school.

Mobile Technologies (including Bring Your Own Device):

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Existing mobile technologies such as gaming devices, mobile and smart phones are very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus can open up risk and misuse associated with communication and internet use. All emerging technologies that the school intends to use will be thoroughly examined and tested before implementation in the classroom. We choose to manage the use of the devices in the following ways so that users exploit them appropriately.

All school owned mobile devices are filtered in the same way as all school computing devices via WebScreen by Atomwide. Pupils are restricted from removing the mobile devices from school

- The school allows staff to bring in personal mobile phones and devices for their own use, they must be switched off during lesson time unless required during an emergency and agreed by the Headteacher. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device.

- Pupils are allowed to bring mobile phones to school but they must be handed in to class teacher upon arrival who then stores the mobile phones in a lockable draw within the classroom. If a pupil is found using them for personal reasons during lessons they will be confiscated.

- The sending of inappropriate text, image and video messages between any member of the school community is not allowed.

- Under no circumstance must content created on the mobile device be uploaded to any web site that shares information i.e. Facebook, Instagram, IChat or YouTube that contains any member of the school community.

- All visitors' mobile phones must be switched off while on school site as detailed in the Visitor safeguarding leaflet.

- The Headteacher has the right to take and examine users' devices in the case of misuse as detailed in the school Behaviour and Relationships Policy.

- Personal mobile phones are not to be used to take and store photographs of pupils even if for school use.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. Such images may provide avenues for cyberbullying 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.

All parents and guardians are asked for permission to use their child's work/photos in the following ways:

- On the school's website
- In the school prospectus and other printed publications that the school may produce for promotional purposes
- Recorded/transmitted on a DVD, video or webcam
- Broadcast on the school's internal multimedia displays
- In display material that may be used in external areas i.e. art exhibitions etc

- General media appearances i.e. local, national media or press releases sent to the press highlighting an activity

This consent form is issued annually to parents at The Three Saints Academy. A copy is also available to parents through Arbour for them to review. Pupil names, email, postal address and mobile numbers will not be published against any image.

Storage of Images

- Images of children and staff are stored securely on the school's network.
- Pupils and staff are not permitted to use personal portable media for storage of images.
- Access to these images are only for the school's staff and pupils for school purposes only and use on the school's website and social media sites.
- The Computing Lead in liaison with Agilysis is responsible for the deletion of images no longer in use by the school or if the member of staff or pupil has left the school.

CCTV/Webcams

- The school has a CCTV infrastructure for the safety and security of all persons on the site. The only people that have access to CCTV real-time viewing are the Office Admin Staff and SLT.
- Any CCTV footage that is captured for security purposes is only available for viewing by the CEO, Headteacher or their nominated Deputy and the Police.

The school will inform and educate users about these risks:

- When using digital images, staff should inform pupils about the risks associated.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press
- parents / carers are not permitted to take videos and digital images of children at school events.
- Staff are allowed to take digital / video images to support educational aims, but must follow this policy concerning the sharing, distribution and publication of those images. Those images should only be taken on St Michael with St Thomas Primary school's 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 St Michael with St Thomas Primary school into disrepute.
- pupils must not take, use, share, publish or distribute images of others without their permission
- 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 parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to GDPR which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

St Michael with St Thomas Primary school ensures that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". (Appendix 8)
- It has a Data Protection Policy
- It is registered as a Data Controller
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out

- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner's Office.

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.
- Use personal data 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.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, once it has been transferred or its use is complete

Communications:

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies St Michael with St Thomas Primary school considers the following as good practice:

- The official Three Saints Academy's email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, 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.
- The School Website has a Need to Talk reporting button for pupils to communicate with school.
- Any digital communication between staff, pupils or parents / carers must be professional in tone and content. These communications may only take place on official (monitored) systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about e-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 St Michael with St Thomas Primary school's website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity:

Refer to the St Michael with St Thomas Primary school's Acceptable Use Agreement and Social Media Policy.

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. St Michael with St Thomas Primary school could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the St Michael with St Thomas Primary school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

St Michael with St Thomas Primary school provides 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

St Michael with St Thomas Primary school's staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or the St Michael with St Thomas Primary school's 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 Academy.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

St Michael with St Thomas Primary school's social media accounts are established and monitored through:

- 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 behavior for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under the Three Saints Academy's 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 St Michael with St Thomas Primary school or impacts on the academy, it must be made clear that the member of staff is not communicating on behalf of the school or the Three Saints Academy with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

- St Michael with St Thomas Primary school permits reasonable and appropriate access to private social media sites

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 effectively respond to social media comments made by others according to our monitored process

St Michael with St Thomas Primary school's use of social media for professional purposes will be checked regularly by the Computing Lead and Agilysis to ensure compliance with the school policies.

Unsuitable / inappropriate activities:

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from St Michael with St Thomas Primary school's 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 /academy context, either because of the age of the users or the nature of those activities.

St Michael with St Thomas Primary school believes that the activities referred to in the following section would be inappropriate in the school's context and that users, as defined below, should not engage in these activities in / or outside school when using our equipment or systems. St Michael with St Thomas Primary school restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by The Three Saints Academy's					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	

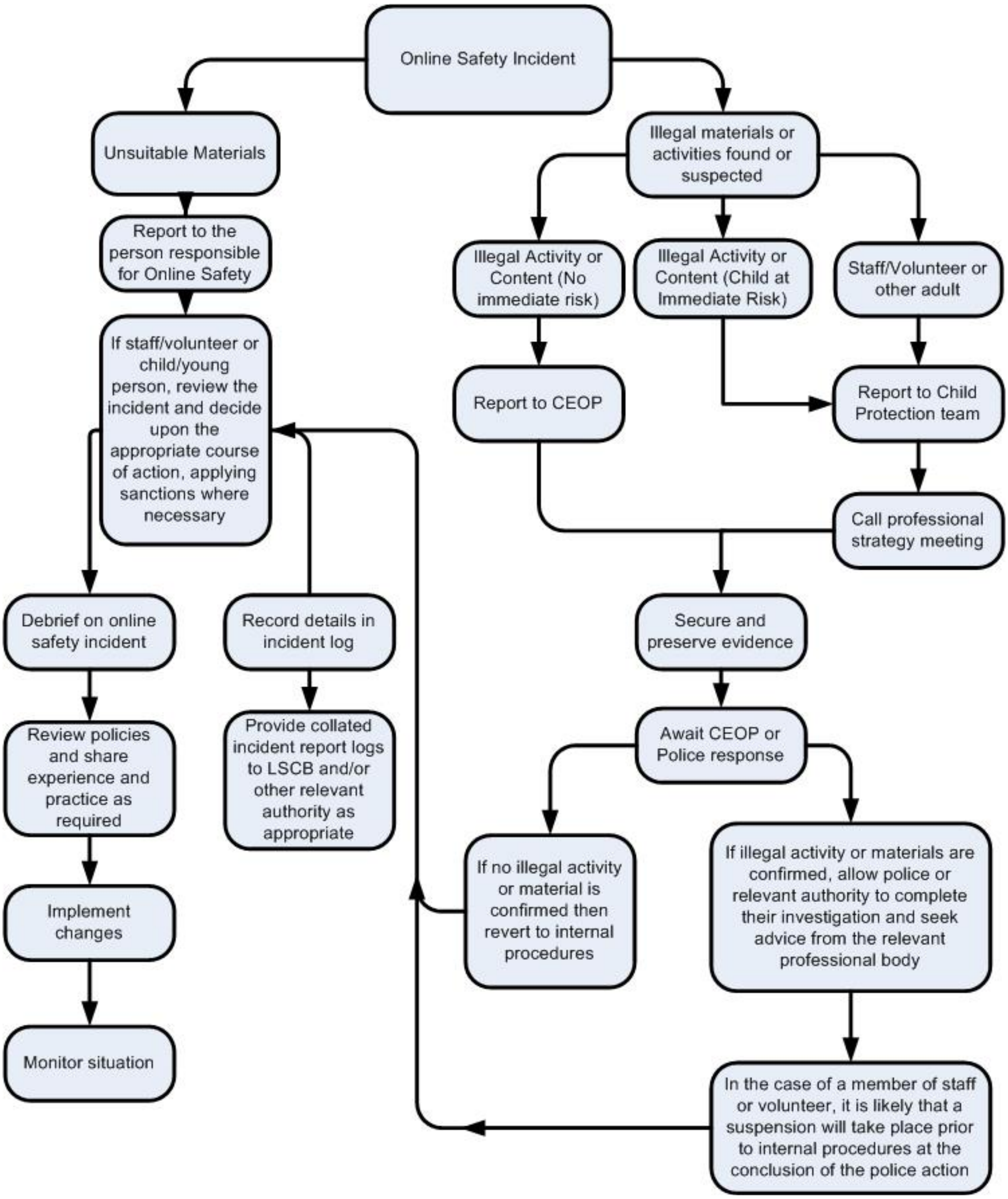
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		X			
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping / commerce				X	
File sharing		X			
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting e.g. Youtube			X		

Responding to incidents of misuse:

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

Illegal Incidents:

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



Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or 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 prior to internal procedures at the conclusion of the police action

Other Incidents:

It is hoped that all members of St Michael with St Thomas Primary school will be responsible users of digital technologies, who understand and follow the school's policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should 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 (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated SLT 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 / Academy Directors or national / local organisation (as relevant).
    - ✓ Police involvement and/or action

- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - ✓ incidents of 'grooming' behaviour
    - ✓ the sending of obscene materials to a child
    - ✓ adult material which potentially breaches the Obscene Publications Act
    - ✓ criminally racist material
    - ✓ promotion of terrorism or extremism

- ✓ other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for St Michael with St Thomas Primary school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the DSP for evidence and reference purposes.

St Michael with St Thomas Primary school's Actions & Sanctions:

St Michael with St Thomas Primary 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:

Pupils Incidents	Refer to class teacher	Refer to Key Stage Leader	Refer to Headteacher / Executive Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Further sanction / exclusion
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
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			X
Unauthorised downloading or uploading of files	X	X	X			X
Allowing others to access the Three Saints Academy's network by sharing username and passwords			X			X
Attempting to access or accessing the Three Saints Academy's network, using another pupil's account			X			X
Attempting to access or accessing the Three Saints Academy's network, using the account of a member of staff			X			X
Corrupting or destroying the data of other users	X					X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X			X
Continued infringements of the above, following previous warnings or sanctions			X			X
Actions which could bring the Three Saints Academy's into disrepute or breach the integrity of the ethos of the school			X			X
Using proxy sites or other means to subvert the school's / academy's filtering system			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

Receipt or transmission of material that infringes the copyright of another person or infringes GDPR			X			X

	Action/Sanctions				
Staff Incidents	Refer to line manager	Refer to Headteacher /Executive Principal	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	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		
Inappropriate personal use of the internet / social media / personal email		X			X
Unauthorised downloading or uploading of files		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
Careless use of personal data e.g. holding or transferring data in an insecure manner		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
Actions which could compromise the staff member's professional standing		X			X
Actions which could bring the Three Saints Academy's into disrepute or breach the integrity of the ethos of the Three Saints Academy		X		X	X

Using proxy sites or other means to subvert the school's / academy's filtering system		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
Breaching copyright or licensing regulations		X			X
Continued infringements of the above, following previous warnings or sanctions		X			X

Appendices

Appendix 1:

St Michael with St Thomas Church of England Primary School

Consent Form

Photographs and Videos

For more information on how we collect and use photographs and video, please refer to our Photo and Video Guidelines available on the school website or from the school office.

We collect and use photographs and videos for the following purposes. Please tick the box to confirm you agree to the use of photographs and videos for that purpose:

Photographs for display in access-controlled areas of the school with child's first name (such as corridors, classrooms)	
Photographs for display in public areas of the school with child's first name (such as reception)	
Photographs for use in the school newsletter and other printed documents that we produce for promotional purposes. (such as the prospectus)	
Photographs for use on the school website	
Photographs for use on social media (such as the school Twitter)	
School photographs provided to the media for publication or broadcast	
For sale of class photographs annually to parents and family members (photos will be shared with yearbook production team)	
Name, Pupil No., Class & Tutor Group will be shared with the external photographer to help with facilitating the purchase of photographs directly from the photographer	
Video recordings of performances, class activities and sporting events in school	
Video recordings of performances, sporting events, activities, and trips out of school	

Off-site activities

Please tick the box to confirm you give consent for your child for that purpose:

To attend supervised visits/sports events to local destinations away from the main school site (includes walking and use of Hired Transport)	
To attend supervised one-day non-residential visits within the UK (These would still be subject to standard school letter/permission slips)	

To attend supervised Swimming off site (Kingsway Leisure Centre) (These would still be subject to standard school letter/permission slips)	

On-site activities

Please tick the box to confirm you give consent for your child for that purpose:

To use the internet in line with the school’s acceptable usage policy	
To take part in food preparation/cooking and tasting activities	
Please outline any food allergies/specific dietary requirements:	

Medical

Please tick the box to confirm you give consent for that purpose:

For my child to be given first aid by a trained member of staff during any on-site or off-site activity	
For my child’s information to be shared with the NHS and other relevant health professionals	
For staff to administer the medicines as specified on signed medication forms to my child	

Home and School Agreement

Please tick the box to confirm you give consent for that purpose:

I have read and understood parents' expectations within the ‘Home and School Agreement’	

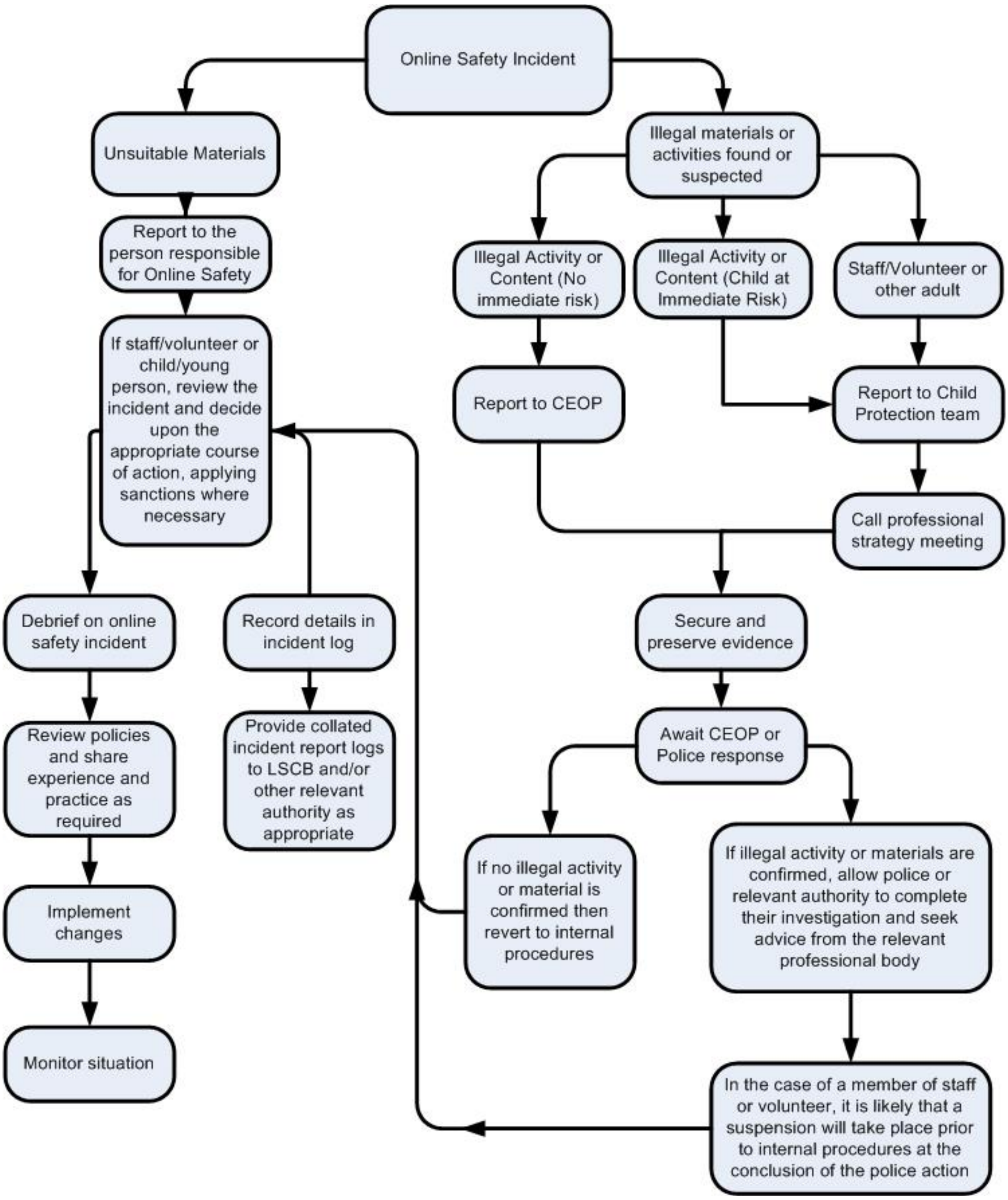
I agree I have read and understood the information.

Pupil name	
Signature of parent/carer*	
Name of parent/carer (if relevant)	
Date:	

If you wish to withdraw consent, please ask the school office for a consent withdrawal form.

Appendix 2:

Responding to incidents of misuse – flow chart



Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or 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 prior to internal procedures at the conclusion of the police action

Appendix 3:

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group: ....

Date: ....

Reason for investigation: ....

....

....

....

Details of first reviewing person

Name: ....

Position: ....

Signature: ....

Details of second reviewing person

Name: ....

Position: ....

Signature: ....

Name and location of computer used for review (for web sites)

....

....

Web site(s) address / device	Reason for concern

Conclusion and Action proposed or taken

Appendix 4:

St Michaels with St Thomas Privacy Notice.

The Three Saints Academy Trust

Data Privacy Notice – Parents & Pupils

GDPR DATA PROTECTION

Data Privacy Notice

Document version control

Version	Author	Date	Approved by	Effective from
1.0 template	DPE - JE	1/5/2018		
2.0	Three Saints	15/5/2018	Directors	15/5/2018
3.0	Kim Sawe	14/10/2020	Management team	14/10/2020

Contents

How we use pupil information

The categories of pupil information that we collect, hold and share include: • Personal information (such as name, unique pupil number and address);

• Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility);

• Attendance information (such as sessions attended, number of absences and absence reasons);

• Assessment information and education records;

• Special Educational Needs information;

• Behavioural information (such as, achievements, exclusions, internal exclusions and detentions);

• Health and medical information (such as dietary requirement and medication details);

• Safeguarding and Child Protection reports and disclosures;

• Photographs and video clips;

• Letters sent to school by parents and carers, letters sent to parent and carers from school

Why we collect and use this information

We use the pupil data:

- to support pupil learning;
- to monitor and report on pupil progress;
- to provide appropriate pastoral care;
- to assess the quality of our services;
- to comply with the law regarding data sharing.

The lawful basis on which we use this information

- We collect and use pupil information under a task performed in the public interest where it relates to a child's educational progression;
- Some photographs and videos are used only after gaining explicit consent;
- Where medical data is being processed, this is processed under a legal obligation (Children and Families Act 2014 which includes a duty on schools to support children with medical conditions);
- Safeguarding data is processed under the legal obligation of The Education Act 2002. Sections 21 and 175 detail how governing bodies of schools must promote the wellbeing of pupils and take a view to the safeguarding of children at the school.
- Children and Families Act 2014 includes a duty on schools to support children with medical conditions;
- The Equality Act 2010 (England, Scotland and Wales) requires you to make reasonable adjustments to ensure that children and young

people with a disability are not put at a substantial disadvantage compared with their peers;

• The Education Act 2002, Sections 21 and 175 detail how governing bodies of schools must promote the wellbeing of pupils and take a view to the safeguarding of children at the school;

• Section 3 of the Children Act 1989 places a duty on a person with the care of a child to do all that is reasonable in the circumstances for the purposes of safeguarding the child;

• Education Act 1996, relating to attendance at school. Collecting pupil information

Whilst most of the pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data

See our Retention Policy for the time periods we hold pupil data.

Who we share pupil information with

We routinely share pupil information with:

• schools that the pupil's attend after leaving us;

• our local authority; social care, education psychology services, speech therapy & speech and language services

• the Department for Education (DfE).

• School Nurse, NHS

- The Three Saints Academy Trust

Why we share pupil information:

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with the (DfE) under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD.

The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-andsupporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis;

- producing statistics;

- providing information, advice or guidance.

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data;

- the purpose for which it is required; • the level and sensitivity of data requested and;

- the arrangements in place to store and handle the data.

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information to, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requestsreceived

To contact DfE: https://www.gov.uk/contact-dfe

Other information we collect and hold:

The categories of other information that we collect, hold and share include:

• Parents' and carers information (such as name, address, contact information, relationship to the child, involvement with volunteer groups or parents association);

• Visitor information (such as name, business, car registration, DBS certification, purpose of visit);

• Governors' information (such as name, address, contact information, business interests, financial interests and governance roles in other schools);

• Volunteers' information (such as name, address, contact information, DBS certification).

• Minutes of meetings

• Letters sent to school by parents and carers, letters sent to parent and carers from school.

Why we collect and use this information

Parents information is collected so that:

- We can communicate with you about your child (in relation to things such as education and attainment, health and well-being, attendance and behaviour);

- Send you important information about the school;

- Provide you with access to tools and services we use in schools (such as parent payment systems, communication applications).

Visitor information is collected so that:

- We have a record of who is and has been in the building, for health, safety and operational purposes;

- We know whether a visitor can be unaccompanied in areas where children are present;

- We have a record of official visits (such as inspections or maintenance).

Governors' information is collected so that:

- We can communicate with Governors on school business;

- There is a public record of Governors and their business interests.

The lawful basis on which we use this information

- Parental information is processed in the public interest where it is related to their child's education.

We may have a legal obligation to process data in certain processing activities and in some circumstances, we will rely on consent as the lawful basis;

• Visitor information is processed as a task in the public interest where it relates to school operations and under a legal obligation where it relates to health and safety;

• Governor information is processed as a task in the public interest. Collecting this information

• Parents: whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain information to us or if you have a choice in this;

• Visitors: As a visitor the information that you provide to us is voluntary. However, we may restrict access to the school if the information is not provided;

• Governors: whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain information to us or if you have a choice in this. Storing this information

We hold school workforce data as documented in our Retention Schedule, which can be requested by contacting the school office.

Who we share this information with

We routinely share this information with:

• Parents: we will share your information with members of staff, other agencies and, where you have agreed, with third-party processors who provide services to the school;

• Visitors: your information will not be shared unless requested by an external agency in the course of a health and safety incident or in the investigation of a crime;

• Governors: we will publish the names, business interests, financial interests and governance roles of governors in other schools on the school website.

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information that we hold about you. To make a request for your personal information, contact the data protection officer whose contact details are at the top of this notice.

You also have the right to:

• object to processing of personal data that is likely to cause, or is causing, damage or distress;

• prevent processing for the purpose of direct marketing; • object to decisions being taken by automated means; • in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed and; • claim compensation for damages caused by a breach of the Data Protection regulations.

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at:

https://ico.org.uk/concerns/

In line with government requirement we are providing online learning for pupils who are unable to attend school because of the coronavirus restrictions.

Type of information we will process

- Personal information (such as name, unique pupil number and address);

- Photographs and video clips;

The lawful basis on which we use this information

- We collect and use pupil information under a task performed in the public interest where it relates to a child's educational progression;

Details

As part of the provision for remote learning we are delivering live lessons to pupils using Microsoft Teams. Live lessons are recorded and uploaded to private class folders on Microsoft Teams to enable fair access to learning for pupils unable to log in to live lessons. Access to the folders is restricted to members of the senior leadership team, class teachers and learning assistants, IT support staff and the pupils in the class.

Appendix 5:

Legislation:

Schools/academies should be aware of the legislative framework under which this online safety policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an online safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

School/academies may wish to view the National Crime Agency website which includes information about "Cyber crime – preventing young people from getting involved". Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with schools to encourage young people to make positive use of their cyber skills. There is a useful summary of the Act on the NCA site.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

The Data Protection Act 2018 (GDPR):

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

- Receive clear information about what you will use their data for.
- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent/carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

For further guidance or support please contact the Revenge Porn Helpline

Appendix 6:

Links to other organisations or documents:

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

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.

<u>Appendix 7:</u>

<u>Staff Acceptable Use Policy:</u>

The Three Saints Academy Trust

Acceptable User Policy

Author/owner: Principals/Directors

Date adopted: 2016

Reviewed: August 2019

Anticipated review: August 2020

Acceptable User Policy

This Acceptable User Policy applies to all staff, pupils and visitors who have access to computers and devices that have access to the internet. Use of the Internet by the fore mentioned users is permitted and encouraged where such use supports the goals and objectives of The Three Saints Academy Trust. Access to the Internet is a privilege and all users must adhere to the policies concerning Computer, Email and Internet usage in line with the Data Protection Act 2018 (GDPR). Violation of these policies could result in disciplinary and/or legal action. All users are required to acknowledge receipt and confirm that they have understood and agree to abide by the rules hereunder and to ensure pupils also abide by these rules.

Computer, email and internet usage

- All users are expected to use the internet responsibly and productively. Internet access on the school's digital hardware resources and systems is limited to work-related activities or for uses deemed 'reasonable' by the Head and/or Governing Body. Personal use is not permitted.

- Work-related activities include research and educational tasks that may be found via the Internet that would help in a user's role.

- All Internet data that is composed, transmitted and/or received by The Three Saints Academy Trust is considered to belong to the trust and is recognised as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties.

- Any equipment, services and technology used to access the Internet on the Trust's domain will be monitored and filtered via the web filtering software.

- Emails sent via the school's approved email system should not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images.

- Use the approved school email system or any other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.

- All sites and downloads are monitored and can be blocked by Agilisys if they are deemed to be harmful.

- All Internet usage / and network usage is logged and this information could be made available to my manager upon request.

- Ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.

- The installation of software must be approved by the Principal.

- Confidential data transported from one location to another must be protected by encryption following the school's data security protocols when using any such data at any location.

Unacceptable use includes, but is not limited to:

- Allowing unauthorised individuals to access email / Internet / network / or other school / LA systems,

- Stealing, using, disclosing someone else's password or sharing your own.

- Engaging in any online activity that may compromise my professional responsibilities.

- Downloading any software or resources from the Internet that can compromise the network or those that are not adequately licensed.

- Knowingly introducing malicious software onto the network.

- Hacking into unauthorised websites.

- Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via St Helens email service.

- Accessing work emails on a personal device (including mobile phone) other than via web-based email systems (web mail).

- Sending or posting information that is defamatory to the company, its products/services, colleagues and/or customers.

- Browsing, downloading or sending material that could be considered offensive.

- Sending or posting chain letters, solicitations, or advertisements not related to Academy purposes or activities.

- Passing off personal views as representing those of the organisation.

- Sharing confidential material, confidential information, or proprietary information outside of The Three Saints Academy Trust.

- Connecting a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software.

- Using personal digital cameras or camera phones for taking and transferring images of pupils or staff.

If a User is unsure about what constitutes Acceptable Internet usage, then he/she should ask his/her ICT Coordinator for further guidance and clarification.

All terms and conditions as stated in this document are applicable to all users of the Agilisys network and Internet connection. All terms and conditions as stated in this document reflect an agreement of all parties and should be governed and interpreted in accordance with the policies and procedures mentioned above. Any user violating these policies is subject to disciplinary actions deemed appropriate by the Directors.

User compliance

I understand and will abide by this Acceptable Usage Policy. I further understand that should I commit any violation of this policy, my access privileges may be revoked, disciplinary action and/or appropriate legal action may be taken.

I agree to have an email account, be connected to the Internet and be able to use the school's ICT resources & systems.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

User Signature

Signature .... Date ....

Full Name .... (printed)

Job title ....

Authorised Signature (Head Teacher)

I approve this user to be set-up.

Signature .... Date ....

Full Name .... (printed)

Appendix 8:

Visitor Acceptable Use Policy.

St Michael with St Thomas

C of E Primary School

Visitors to School Policy

Author: Headteacher

Owner: School Committee/CEO

Date adopted: December 2019

Review: December 2022

We are a rights respecting school. All our policies and procedures are written and reviewed to ensure that children's rights, as detailed in the United Nations Convention on the Rights of the Child, are respected and promoted and this policy ensures:

Article 19: All children should be protected from violence, abuse and neglect, and governments should protect them.
Article 32: Children should not be allowed to do work that is dangerous or might make them ill, or stop them going to school.
Article 37: No child should be punished in a way that humiliates or hurts them.
Article 12: All children have a right to be able to give their opinion when adults are making a decision that will affect them, and adults should take it seriously.
Article 29: Education should help children use and develop their talent and abilities. It should also help children learn to live peacefully, protect the environment and respect other people.

For more information on the convention and the rights of each child visit: http://www.unicef.org.uk/

Visitors to School Policy

Overview

The safety of our children is paramount. This policy has been put in place to ensure that visitors to our school are carefully checked and monitored during their time here. This will ensure that no unauthorised person has entry to the school.

Aims of the policy

The purpose of this policy and its associated procedures is to contribute towards the safeguarding of all children and staff both during and outside of school hours when they are on our site. The ultimate aim is to ensure that all children and staff learn and work in an environment where they are safe and free from harm by:

1. Preventing unauthorised persons from entering school
2. Making visitors welcome
3. Ensuring that visitors are monitored and checked
4. Monitoring visitors carefully during their time in school
5. Being able to account for, and locate, visitors at all times

We have responsibility for the safety and well-being of all of our children anywhere on the school site, during normal school hours, during after school activities and on school organised (and supervised) off-site activities.

This policy applies to:

- Pupils
- All teaching and non-teaching staff employed by the school
- All external visitors entering the school site during the school day or for after school activities (including peripatetic tutors, sports coaches etc)
- Governors
- Parents/carers
- Volunteers
- Children
- Local Authority visiting staff e.g. EP, Inclusion Officer
- Visiting support staff e.g. school nurse, SALT
- Building & Maintenance Contractors

Visitors Invited to the School

Before a visitor is invited to the school, the Head teacher is informed, with a clear explanation as to the relevance, purpose date and time of the visit. Permission must be granted by the Head teacher before a visitor is asked to come into school.

Managing Visitors

1. External doors will be kept securely closed and external signs will direct visitors to the main entrance and reception desk
2. All visitors will report to the school reception desk where they will be welcomed and asked for their details and for the name of the person they need to see
3. Visitors must sign-in on Inventry and sign out as they leave
4. Formal visitors representing the LA, businesses, contractors, outside agencies etc. are required to present formal identification
5. Each visitor will be given an identification that must be worn visibly at all times
6. Visitors' identification badges must be collected in by the office staff before the visitor leaves
7. Visitors will be asked to wait in the reception area until the person that they have come to see arrives to take charge of them. That person will be responsible for them during their time in school and will escort them back to reception at the end of their visit

8. Visitors will be accompanied, or supervised, during the whole of their time in school
9. The Premises Manager will be responsible for work people, and trades people, during their time in school. They must show proof of identity to the site supervisor if they are not already known to him/her. He/she will alert senior staff of their presence
10. The headteacher must be informed immediately if members of the police, fire service, local authority, Ofsted, or other official bodies, arrive at school unexpectedly
11. Any visitor to the school site who is not wearing an identity badge is challenged politely to enquire who they are and their business on the school site. They should then be escorted to reception to sign the visitors' book and be issued with an identity badge. The above procedures then apply.
12. In the event that the visitor refuses to comply, they are asked to leave the site immediately and the Head teacher informed. The Head teacher (or Senior Leader if HT not available) will consider the situation and decide if it is necessary to inform the police.
13. If any visitor behaves in an unacceptable or threatening manner, they will be required to leave and escorted from the premises immediately. In this situation, they should be immediately removed from any situations where there is a possibility of them harming children or staff. If necessary, the police should be summoned to remove them
14. All visitors arriving to the school for the first time, are issued with a leaflet outlining key safeguarding and health and safety related information (***please read this policy in conjunction with the Visitors' Leaflet)***

Governors and Long-Term Volunteers

All governors and long-term volunteers are required to have an enhanced DBS. New governors are made aware of this policy and are expected to become familiar with its procedures as part of their induction. This is the responsibility of the Head teacher and the Chair of Governors or Training Liaison Governor.

New volunteers will be asked to comply with this policy when first coming into school for an activity or class supporting role.

At lunchtime, visitors/volunteers will not use the staffroom, but will be taken to the meeting room/HT office for the duration of lunchtime and will be collected again following lunch by the member of staff responsible for them.

Short Term visitors

All short-term visitors who are on site without DBS are never left unattended and they must be supervised by a member of staff at all times.

CPD

As part of their induction, new staff are made conversant with this policy for visitors and asked to ensure compliance with its procedures at all times.

Monitoring and Evaluation

The suitability of all visitors invited into school to work with our children is assessed at the end of their visit and a decision made as to whether they may be asked to visit the school in future.

Annex 1

COVID-19 school closure arrangements for Safeguarding and Child Protection at

St Michael with St Thomas CE Primary School-

The Three Saints Academy

School Name: St Michael with St Thomas CE Primary School- The Three Saints Academy

Policy owner: CEO/Director of Wellbeing

Date: 30 March 2020

Date shared with staff: 30 March 2020

1. Context

From 20th March 2020 parents were asked to keep their children at home, wherever possible, and for schools to remain open only for those children of workers critical to the COVID-19 response - who absolutely need to attend.

Schools and all childcare providers were asked to provide care for a limited number of children - children who are vulnerable, and children whose parents are critical to the COVID-19 response and cannot be safely cared for at home.

This addendum of the St Michael with St Thomas CE Primary School -The Three Saints Academy Safeguarding and Child Protection policy contains details of our individual safeguarding arrangements in the following areas:

Key contacts

Role	Name	Email
Designated Safeguarding Lead/Headteacher	Michelle Slingsby	Michelle.slingsby@three-saints.org.uk
Deputy Designated Safeguarding Leads	Janette Crosbie	Janette.crosbie@three-saints.org.uk
Chair of Governors	Lesley Traves	Lesley.traves@three-saints.org.uk
Safeguarding Governor	Lesley Traves	Lesley.traves@three-saints.org.uk
CEO	Kirsty Tennyson	Kirsty.tennyson@three-saints.org.uk
Director of Wellbeing	Linda Smith	Linda.smith@three-saints.org.uk

Vulnerable children

Vulnerable children include those who have a social worker and those children and young people up to the age of 25 with education, health and care plans (EHCP).

Those who have a social worker include children who have a Child Protection Plan and those who are looked after by the Local Authority. A child may also be deemed to be vulnerable if they have been assessed as being in need or otherwise meet the definition in section 17 of the Children Act 1989.

Those with an EHCP plan will be risk-assessed in consultation with the Local Authority and parents, to decide whether they need to continue to be offered a school or college place in order to meet their needs, or whether they can safely have their needs met at home. This could include, if necessary, carers, therapists or clinicians visiting the home to provide any essential services. Many children and young people with EHC plans can safely remain at home.

Eligibility for free school meals in and of itself should not be the determining factor in assessing vulnerability. The Designated Safeguarding Lead (and deputy) have identified the most vulnerable children. They have the flexibility to offer a place to those on the edge of receiving children's social care support.

St Michael with St Thomas CE Primary School, The Three Saints Academy will continue to work with and support children's social workers to help protect vulnerable children. This includes working with and supporting children's social workers and the local authority virtual school head (VSH) for looked-after and previously looked-after children. The lead person for this will be the Headteacher – Michelle Slingsby.

There is an expectation that vulnerable children who have a social worker will attend an education setting, so long as they do not have underlying health conditions that put them at increased risk or other significant reasons. In circumstances where a parent does not want to bring their child to an education setting, and their child is considered vulnerable, the social worker and St Michael with St Thomas CE Primary School, The Three Saints Academy will explore the reasons for this directly with the parent.

Where parents are concerned about the risk of the child contracting COVID19, St Michael with St Thomas CE Primary School, The Three Saints Academy or the social worker will talk through these anxieties with the parent/carer following the advice set out by Public Health England.

St Michael with St Thomas CE Primary School, The Three Saints Academy will encourage our vulnerable children and young people to attend a school, including remotely if needed.

Attendance monitoring

Schools do not need to complete their usual day-to-day attendance processes to follow up on non-attendance.

If St Michael with St Thomas CE Primary School ,The Three Saints Academy has any children in attendance (e.g. because they are vulnerable or their parent(s) / carers are critical workers) we will submit the daily attendance sheet to the DfE by 12 noon - https://www.gov.uk/government/publications/coronavirus-covid-19-attendance-recording-for-educational-settings

If the school has closed, we will complete the return once as requested by the DfE.

St Michael with St Thomas CE Primary School, The Three Saints Academy and social workers will agree with parents/carers whether children in need should be attending school. St Michael with St Thomas

CE Primary School, The Three Saints Academy will then follow up on any pupil that they were expecting to attend, who does not. St Michael with St Thomas CE Primary School, The Three Saints Academy will also follow up with any parent or carer who has arranged care for their child(ren) and the child(ren) subsequently do not attend.

To support the above, St Michael with St Thomas CE Primary School, The Three Saints Academy will, when communicating with parents/carers and carers, confirm emergency contact numbers are correct and ask for any additional emergency contact numbers where they are available.

In all circumstances where a vulnerable child does not take up their place at school, or discontinues, St Michael with St Thomas CE Primary School, The Three Saints Academy will notify their social worker. Every child identified as meeting criteria for a school place but does not take up a place will be contacted three times a week by the DDL/DDSL if CP or CiN and at least once a week for any other vulnerable pupil.

Designated Safeguarding Lead

St Michael with St Thomas CE Primary School, The Three Saints Academy has a Designated Safeguarding Lead (DSL) and a Deputy DSL.

The Designated Safeguarding Lead is: Michelle Slingsby

The Deputy Designated Safeguarding Lead is: Janette Crosbie

The optimal scenario is to have a trained DSL (or deputy) available on site. Where this is not the case a trained DSL (or deputy) will be available to be contacted via phone - for example when working from home.

Where a trained DSL (or deputy) is not on site, in addition to the above, a senior leader will assume responsibility for co-ordinating safeguarding on site.

This might include updating and managing access to child protection online management system, CPOMS and liaising with the offsite DSL (or deputy) and as required liaising with children’s social workers where they require access to children in need and/or to carry out statutory assessments at school.

It is important that all St Michael with St Thomas CE Primary School, The Three Saints Academy staff and volunteers have access to a trained DSL (or deputy). On each day, the staff on site will be made aware of who that person is and how to contact them.

The DSL will continue to engage with social workers, and attend all multi-agency meetings, which can be done remotely.

Reporting a concern

Where staff have a concern about a child, they should continue to follow the process outlined in the school Safeguarding Policy, this includes making a report via CPOMS, which can be done remotely.

In the unlikely event that a member of staff cannot access their CPOMS from home, they should email the Designated Safeguarding Lead/Headteacher, Deputy DSL. This will ensure that the concern is received.

Staff are reminded of the need to report any concern immediately and without delay.

Where staff are concerned about an adult working with children in the school, they report the concern to the headteacher.

Concerns around the Headteacher should be directed to the CEO: Kirsty Tennyson or Chair of Governors: Lesley Traves.

Safeguarding Training and induction

DSL training is very unlikely to take place whilst there remains a threat of the COVID 19 virus.

For the period COVID-19 measures are in place, a DSL (or deputy) who has been trained will continue to be classed as a trained DSL (or deputy) even if they miss their refresher training.

All existing school staff have had safeguarding training and have read part 1 of Keeping Children Safe in Education (2019). The DSL should communicate with staff any new local arrangements, so they know what to do if they are worried about a child.

Where new staff are recruited, or new volunteers enter St Michael with St Thomas CE Primary School, The Three Saints Academy, will continue to be provided with a safeguarding induction.

If staff are deployed from another education or children's workforce setting to our school, we will take into account the DfE supplementary guidance on safeguarding children during the COVID-19 pandemic and will accept portability as long as the current employer confirms in writing that:-

- the individual has been subject to an enhanced DBS and children's barred list check

- there are no known concerns about the individual's suitability to work with children

- there is no ongoing disciplinary investigation relating to that individual

For movement within the Trust, schools should seek assurance from the Multi-Academy Trust (MAT) CEO/Director of Wellbeing, that the member of staff has received appropriate safeguarding training.

Upon arrival, they will be given a copy of the receiving setting's child protection policy, confirmation of local processes and confirmation of DSL arrangements.

Safer recruitment/volunteers and movement of staff

It remains essential that people who are unsuitable are not allowed to enter the children's workforce or gain access to children. When recruiting new staff, St Michael with St Thomas CE Primary School, The Three Saints Academy will continue to follow the relevant safer recruitment processes for their setting, including, as appropriate, relevant sections in part 3 of Keeping Children Safe in Education (2019) (KCSIE).

In response to COVID-19, the Disclosure and Barring Service (DBS) has made changes to its guidance on standard and enhanced DBS ID checking to minimise the need for face-to-face contact.

If staff are deployed from another education or children's workforce setting to our school, the CEO will take into account the DfE supplementary guidance on safeguarding children during the COVID-19 pandemic and will accept portability as long as the current employer confirms in writing that:-

- the individual has been subject to an enhanced DBS and children's barred list check
- there are no known concerns about the individual's suitability to work with children
- there is no ongoing disciplinary investigation relating to that individual

Where St Michael with St Thomas CE Primary School, The Three Saints Academy are utilising volunteers, we will continue to follow the checking and risk assessment process as set out in paragraphs 167 to 172 of KCSIE. Under no circumstances will a volunteer who has not been checked be left unsupervised or allowed to work in regulated activity.

St Michael with St Thomas CE Primary School, The Three Saints Academy will continue to follow the legal duty to refer to the DBS anyone who has harmed or poses a risk of harm to a child or vulnerable adult. Full details can be found at paragraph 163 of KCSIE.

Whilst acknowledging the challenge of the current National emergency, it is essential from a safeguarding perspective that any school is aware, on any given day, which staff/volunteers will be in the school or college, and that appropriate checks have been carried out, especially for anyone engaging in regulated activity. As such, St Michael with St Thomas CE Primary School, The Three Saints Academy will continue to keep the single central record (SCR) up to date as outlined in paragraphs 148 to 156 in KCSIE.

Online safety in schools and colleges

St Michael with St Thomas CE Primary School, The Three Saints Academy will continue to provide a safe environment, including online. This includes the use of an online filtering system.

Where pupils are using computers in school, appropriate supervision will be in place.

Children and online safety away from school and college

It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Child Protection Policy and where appropriate referrals should still be made to children's social care and as required, the police.

Online teaching should follow the same principles as set out in the MAT code of conduct.

St Michael with St Thomas CE Primary School, The Three Saints Academy will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

Below are some things to consider when delivering virtual lessons, especially where webcams are involved:

- No 1:1s, groups only
- Staff and children must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be blurred.
- The live class should be recorded so that if any issues were to arise, the video can be reviewed.
- Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day.
- Language must be professional and appropriate, including any family members in the background.
- Staff must only use platforms specified by senior managers and approved by our IT network manager / provider to communicate with pupils
- Staff should record, the length, time, date and attendance of any sessions held.

Supporting children not in school

St Michael with St Thomas CE Primary School, The Three Saints Academy is committed to ensuring the safety and wellbeing of all its Children and Young people.

Where the DSL has identified a child to be on the edge of social care support, or who would normally receive pastoral-type support in school, they should ensure that a robust communication plan is in place for that child or young person.

All communication must be recorded on CPOMS.

The communication plans can include; phone, text and email contact. Other individualised contact methods should be considered and recorded.

St Michael with St Thomas CE Primary School, The Three Saints Academy and its DSL will work closely with all stakeholders to maximise the effectiveness of any communication plan.

This plan must be reviewed regularly and where concerns arise, the DSL will consider any referrals as appropriate.

The school will share safeguarding messages on its website and social media pages.

St Michael with St Thomas CE Primary School, The Three Saints Academy recognises that school is a protective factor for children and young people, and the current circumstances, can affect the mental health of pupils and their parents/carers. Staff at St Michael with St Thomas CE Primary School, The Three Saints Academy need to be aware of this in setting expectations of pupils' work where they are at home.

Supporting children in school

St Michael with St Thomas CE Primary School, The Three Saints Academy is committed to ensuring the safety and wellbeing of all its students.

St Michael with St Thomas CE Primary School, The Three Saints Academy will continue to be a safe space for all children to attend and flourish. The Headteacher will ensure that appropriate staff are on site and staff to pupil ratio numbers are appropriate, to maximise safety.

St Michael with St Thomas CE Primary School, The Three Saints Academy will refer to the Government guidance for education and childcare settings on how to implement social distancing and continue to follow the advice from Public Health England on handwashing and other measures to limit the risk of spread of COVID19.

St Michael with St Thomas CE Primary School, The Three Saints Academy will ensure that where we care for children of critical workers and vulnerable children on site, we ensure appropriate support is in place for them.

Where St Michael with St Thomas CE Primary School, The Three Saints Academy has concerns about the impact of staff absence – such as our Designated Safeguarding Lead or first aiders – we will discuss them immediately with the CEO of the MAT.

Peer on Peer Abuse

St Michael with St Thomas CE Primary School, The Three Saints Academy recognises that during the closure a revised process may be required for managing any report of such abuse and supporting victims**.**

Where a school receives a report of peer on peer abuse, they will follow the principles as set out in part 5 of KCSIE and of those outlined within our Child Protection Policy.

The school will listen and work with the young person, parents/carers and any multi-agency partner required to ensure the safety and security of that young person.

Concerns and actions must be recorded on CPOMS and appropriate referrals made.

Support from the Multi-Academy Trust

The Multi-Academy Trust (MAT) will provide support and guidance as appropriate to enable the DSL to carry out their role effectively.

This includes, remotely accessing CPOMS records for the purpose of quality assurance, support, guidance and direction.

https://www.gov.uk/government/publications/covid-19-safeguarding-in-schools-colleges-and-other-providers/coronavirus-covid-19-safeguarding-in-schools-colleges-and-other-providers

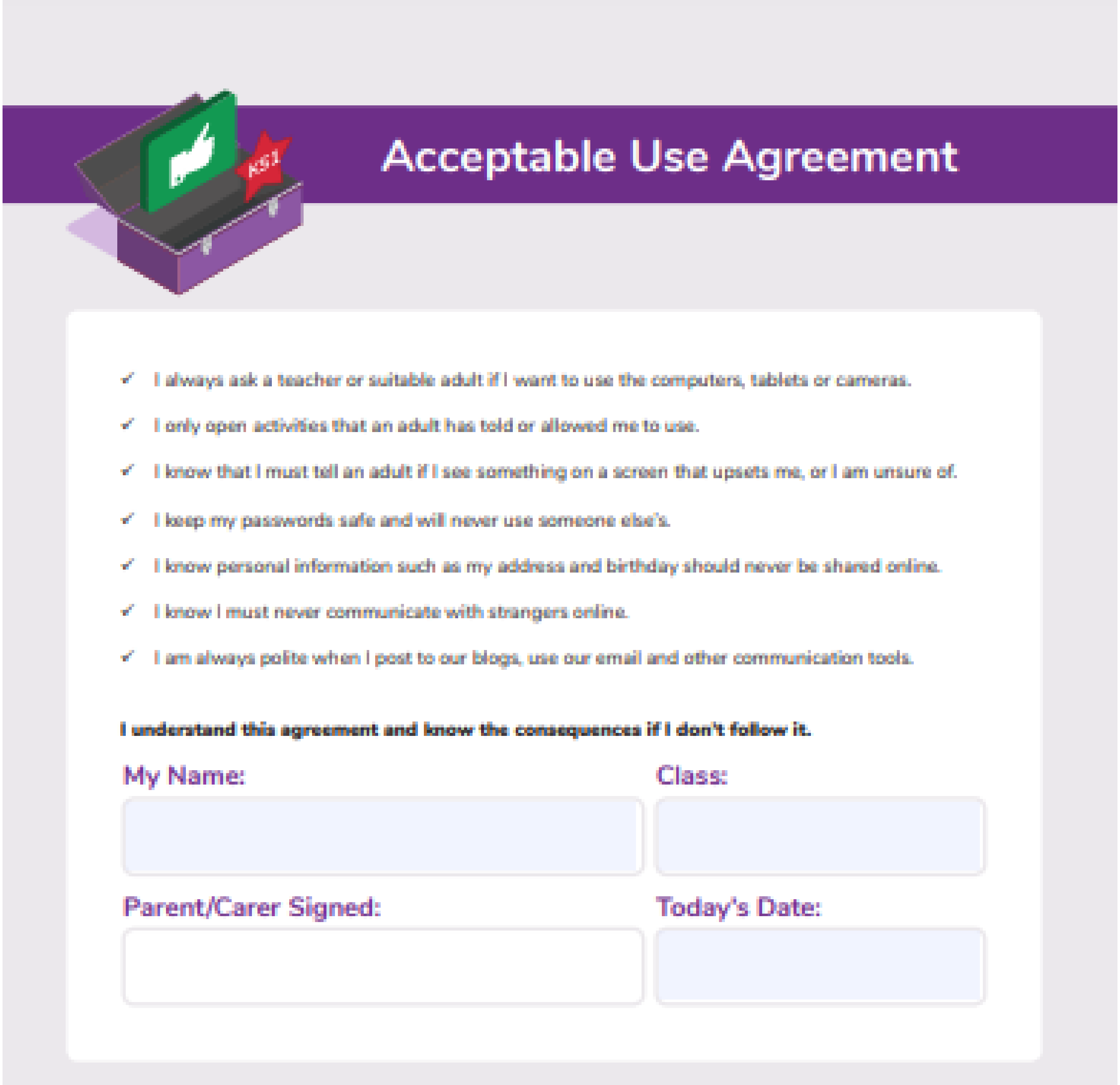
Appendix 9:

Children’s AUP (EYFS, KS1, KS2)

Acceptable Use Agreement
KS1

Type date

Computing Leader



Acceptable Use Agreement

- ✓ I always ask a teacher or suitable adult if I want to use the computers, tablets or cameras.
- ✓ I only open activities that an adult has told or allowed me to use.
- ✓ I know that I must tell an adult if I see something on a screen that upsets me, or I am unsure of.
- ✓ I keep my passwords safe and will never use someone else's.
- ✓ I know personal information such as my address and birthday should never be shared online.
- ✓ I know I must never communicate with strangers online.
- ✓ I am always polite when I post to our blogs, use our email and other communication tools.

I understand this agreement and know the consequences if I don't follow it.

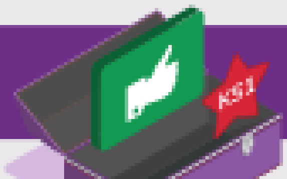
My Name:

Class:

Parent/Carer Signed:

Today's Date:

2simple
KS1



Acceptable Use Agreement

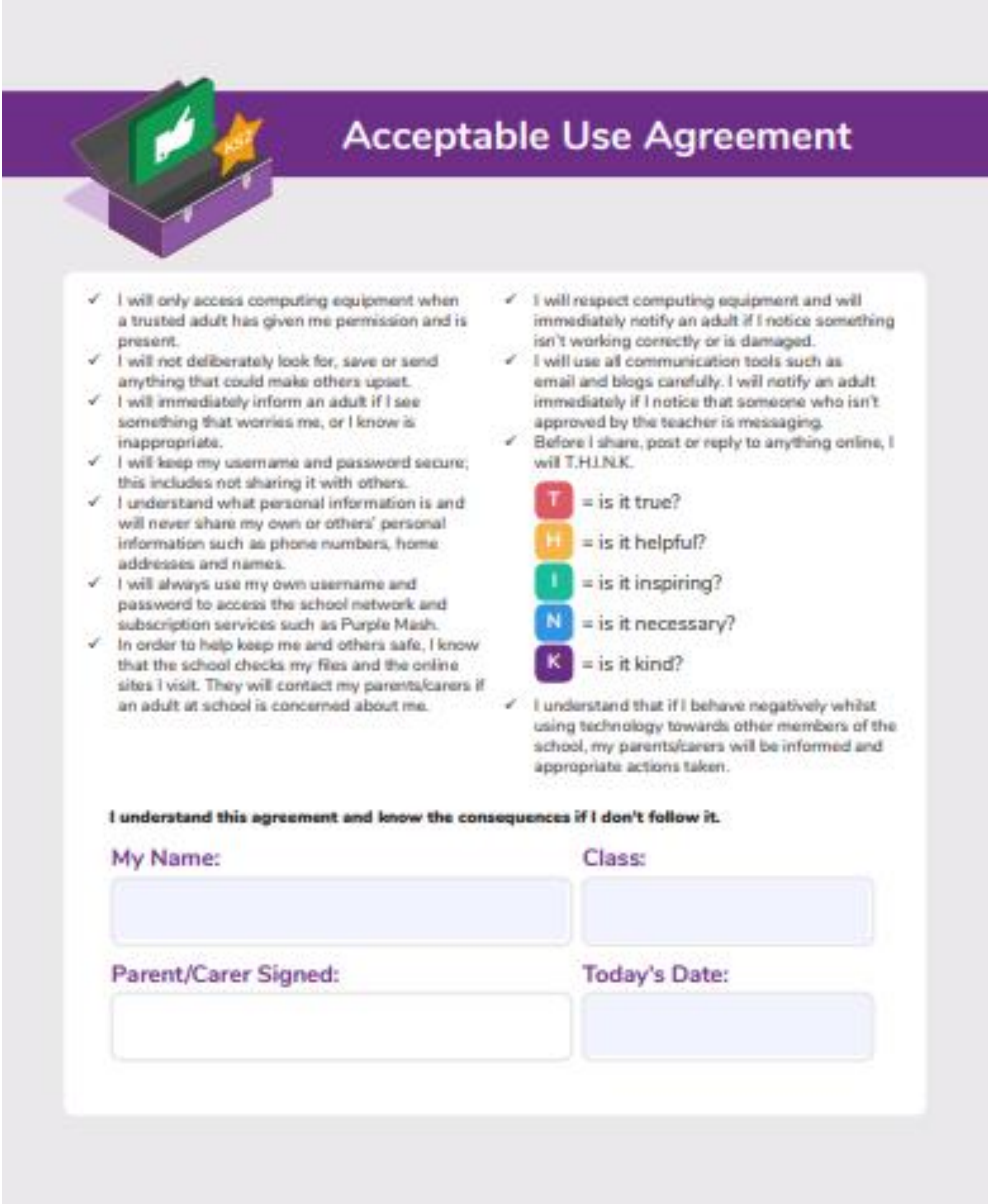
2simple

Acceptable Use Agreement KS2

Type date

Computing Leader

Type name here



Acceptable Use Agreement

- ✓ I will only access computing equipment when a trusted adult has given me permission and is present.
- ✓ I will not deliberately look for, save or send anything that could make others upset.
- ✓ I will immediately inform an adult if I see something that worries me, or I know is inappropriate.
- ✓ I will keep my username and password secure; this includes not sharing it with others.
- ✓ I understand what personal information is and will never share my own or others' personal information such as phone numbers, home addresses and names.
- ✓ I will always use my own username and password to access the school network and subscription services such as Purple Mash.
- ✓ In order to help keep me and others safe, I know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.
- ✓ I will respect computing equipment and will immediately notify an adult if I notice something isn't working correctly or is damaged.
- ✓ I will use all communication tools such as email and blogs carefully. I will notify an adult immediately if I notice that someone who isn't approved by the teacher is messaging.
- ✓ Before I share, post or reply to anything online, I will T.H.I.N.K.

T = is it true?

H = is it helpful?

I = is it inspiring?

N = is it necessary?

K = is it kind?

- ✓ I understand that if I behave negatively whilst using technology towards other members of the school, my parents/carers will be informed and appropriate actions taken.

I understand this agreement and know the consequences if I don't follow it.

My Name:

Class:

Parent/Carer Signed:

Today's Date:

Appendix 10 :

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.