The Cam Academy Trust IT AND Online Safety Policy	
Approved in conjunction with the Audit & Risk Committee on behalf of the Trust Board	27.02.2024
To be reviewed:	Every 2 years or as appropriate
Date of next review:	February 2026
Responsible Officer:	Director of IT Strategy
Category - 1	Version 2

Contents:

1: Background

1.1 Rationale

The CAM Academy Trust recognises that technology has become integral to the lives of children, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. The use of these exciting and innovative tools in schools and at home has been shown to raise educational standards and promote pupil achievement. However, the same new technologies can put young people at risk within and outside school. Trust schools have a duty to ensure that all pupils are able to use the internet and related communications technologies appropriately and safely.

The purpose of the Trust online safety policy is to:

- Clearly identify the key principles and responsibilities of all members of each school's community with regards to the safe and responsible use of technology to ensure that school is a safe and secure environment.
- Safeguard and protect all members of each school's community online, fulfilling the requirements of Keeping Children Safe in Education (KCSiE).
- Raise awareness with all members of each school's community of the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the schools' community.

1.2 The Scope of the Policy

The Trust online safety policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school IT systems, both in and out of school. It also applies to the use of personal digital technology on the school site (where allowed). It outlines the commitment of The Cam Academy Trust to safeguard members of our school communities online in accordance with statutory guidance and best practice.

KCSiE 2023 places a number of responsibilities on schools and school staff with regards to the safety of users of school (and personal) devices both inside and outside of school and this policy seeks to address these issues alongside other areas of online safety.

1.3 Associated Policies

This policy is closely related to a number of other Trust and school frameworks and policies in the following areas:

- Acceptable Use (Staff and Pupils)
- Child Protection and Safeguarding
- ICT Infrastructure / Security
- GDPR
- Behaviour & Discipline
- Mobile Devices

A full list of Trust policies and policy frameworks can be found at https://www.catrust.co.uk/key-information/policies

Schools should be aware of the legislative framework under which this online safety policy framework 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. Any action taken by a school must be in line with relevant Trust/school policies and in line with appropriate legislation and DfE guidance.

2: Roles and Responsibilities

2.1 The Trust Board and Local Governing Bodies

The Trust board has overall responsibility for approval of the online safety policy and for reviewing the effectiveness of this policy. Local Governing Bodies are responsible for monitoring and the implementation of this policy at a local school level. A member of each Governing body will be nominated as the take on the role of Online Safety Governor (this may be as part of the wider safeguarding role), to include:

- regular meetings with the Designated Safeguarding Lead / Online Safety Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training) is taking place as intended
- ensuring that the filtering and monitoring provision is reviewed by the school annually or in the event of significant changes, and that this is recorded.
- reporting to relevant governors group/meeting

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

2.2 Head Teacher

The Headteacher is responsible for:

- ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, although the day-to-day responsibility for online safety will be delegated to a named member of staff.
- ensuring that the filtering and monitoring technology used at their school is appropriate for their setting and context – in this respect they will work with the trust safeguarding lead and IT operations manager.
- ensuring that all staff with responsibility for online safety carry out their responsibilities effectively and receive suitable CPD to enable them to carry out their roles and to train other colleagues, as relevant
- receiving and reviewing regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- working with the responsible Governor, the designated safeguarding lead (DSL) and trust IT operations manager / team in all aspects of filtering and monitoring.
- ensuring that they and at least one other member of their staff (typically a senior leader) are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- liaising with relevant curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated.

2.3 Trust IT Operations Manager

The Trust IT Operations Manager (overseeing the IT Team) is responsible for:

- providing technical advice to school leaders and DSLs to help them ensure that procured ICT filtering and monitoring is fit for purpose.
- ensuring that the Trust / school's IT infrastructure is secure and is not open to misuse or malicious attack.
- ensuring that the school meets the online safety technical requirements outlined in the

Acceptable Use Policy (AUP) and any relevant external policies and guidance.

- ensuring that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.
- there is clear, safe, and managed control of user access to networks and devices.
- ensuring that the school's filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- ensuring that the use of the network, cloud-based systems, remote access, email and any other IT system is regularly monitored in order that any misuse / attempted misuse can be logged and reported to the Online safety lead for investigation / action / sanction.

2.4 The Designated Safeguarding Lead

The key responsibilities of the Designated Safeguarding Lead at each school include:

- holding the lead responsibility for online safety, within their safeguarding role.
- acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
- ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and that all incidents are recorded.
- liaising with the local authority and other local and national bodies, as appropriate.
- keeping up to date with current research, legislation and trends regarding online safety.
- being aware of how the school employs filtering and monitoring, how these systems report or flag potential issues, and how to follow these up.
- maintaining a record of online safety concerns/incidents and actions taken as part of the school's safeguarding recording structures and mechanisms.
- monitoring the school online safety incidents to identify gaps/trends and use this data to update the school's education response to reflect need.
- maintaining a record of any changes requested to the filtering – ie unblocked sites – and the reason(s) why.
- regularly (suggested termly) testing that the current filtering is working as expected, for example using a test pupil account.
- meeting with and reporting to the school's SLT, Governors and other agencies as appropriate, regarding current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out

The DSL should be regularly trained in online safety issues and be aware of the potential for serious child protection 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

2.5 The School Online Safety Lead*:

**Where the school has a separate Online Safety Lead – if not these roles fall within the DSL post and should be added to the DSL role above.*

The online Safety Lead takes day to day responsibility for online safety issues and will:

- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- ensure that all staff are aware of the procedures that need to be followed in the event of an

online safety incident taking place and the need to immediately report those incidents
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- liaise with (school/local authority/trust/external provider) technical staff, pastoral staff and support staff (as relevant)
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education: content, contact, conduct and commerce.

2.6 Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- they understand that online safety is a core part of safeguarding
- they have an up-to-date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the trust Staff Acceptable Use Policy (AUP)
- they immediately report any suspected misuse or problem to the online safety lead / IT helpdesk as per school procedures for a safeguarding or technical issue.
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they support the school in educating pupils about safe use of ICT and that online safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and are encouraged to follow the trust online safety and Acceptable Use Policy (AUP)
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor IT activity (particularly internet use) in lessons, extra-curricular and extended school activities and any breach of the Pupil Acceptable Use Policy (AUP) is dealt with appropriately.
- any deficiencies in the school internet filter are reported immediately
- any online resources (webpages, videos etc) are checked prior to use to ensure they are appropriate for the age group concerned
- they are aware of issues related to the use of personal mobile devices and that they monitor their use and implement current school practices and policies with regard to these devices
- they follow the Trust guidance on Remote Online Working and the Delivery of Live Sessions
- all digital communications with pupils should be on a professional level and only carried out using official school systems
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

2.7 Pupils

- are responsible for using the school IT systems in accordance with the pupil AUP, which they will be expected to sign before being given access to school systems
- need to follow trust and school guidance on remote online working and attending live sessions
- 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 school policies on the use of personal mobile devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying
- should know what to do if they or someone they know feels vulnerable when using online

technology

- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school
- need to have an age-appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

2.8 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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of IT than their children. The school will take every opportunity to help parents understand these issues and reinforce good practice through:

- signposting access to this policy via the policies page on the trust website
- making AUP agreements avilable via their website
- publishing information about appropriate use of social media relating to posts concerning the school
- seeking their permissions concerning digital images, cloud services etc
- sharing relevant information about online safety from third parties

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school.
- supporting the safe and responsible use of school devices at home
- supporting schools with their mobile device policies

2.9 Community Users

Community Learners do not have access to school IT systems. Community tutors who need to access school systems, eg to show a video, use a generic account and sign a Trust AUP before access is granted. As with other groups, usage is tracked via Smoothwall Monitor and filtered at pupil level.

3: Education and Training

3.1 Education – pupils

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

Schools will be able to demonstrate how they teach pupils to use IT equipment safely, in an age and understanding-appropriate way, including to those pupils with SEND. This will be through one or more of the following: timetabled lessons, assemblies, pastoral activities, 1:1 sessions.

A planned online safety programme will have content which is up to date and relevant to all of the pupils who are receiving it, including Yr12/13 and SEND pupils:

- Lessons will be context-relevant with agreed objectives leading to clear and evidenced outcomes. Digital competency will be effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc.
- Content will cover both the use of IT and new technologies in school and outside school.
- Schools will incorporates/make use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.

In addition, online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of IT across the curriculum:

- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of IT, the internet and mobile devices both within and outside school. Rules for use of IT systems and the internet will be posted in all rooms and displayed on log-on screens periodically.
- 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 or if pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the pupils visit.
- Where research is planned as a homework task, it is best practice that pupils should be guided to sites checked as suitable for their use.
- 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.
- It is accepted that from time to time, for good educational reasons, pupils may need to research sensitive topics e.g., racism, drugs, and discrimination. Where this is the case staff should be vigilant in monitoring the content of the websites the pupils visit.

Finally, staff should act as good role models in their use of IT, the internet and mobile devices.

3.2 Education – parents / carers

Parents and carers may have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents can underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about

how to respond. Each school will take every opportunity to help parents understand these issues and reinforce good practice through communication, awareness-raising and engagement using the school newsletter and website to inform about online safety issues, curriculum activities and reporting routes. They will also seek to publicise relevant high profile events / campaigns eg safer internet day.

3.3 Training – Staff

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

- A planned programme of online safety and data protection training will be made available to staff that is relevant and appropriate to their role. An integral part of the school's annual safeguarding and data protection training for all staff, this will be regularly reviewed and updated (where required) in light of changes to legislation / guidance.
- A record of the online safety training of all staff will be kept.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It will include explicit reference to:
    - classroom management
    - professional conduct
    - the need to and the process for reporting any actual / potential online safety incident to the online safety lead in the local school for logging
    - online reputation
    - the need to model positive online behaviours.
- The online safety lead and will receive regular updates through attendance at information and training sessions and by reviewing guidance documents released by Internet provider and others.
- Schools will ensure that staff are aware of the contents of this online safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The online safety lead will provide additional advice / guidance / training as required to individuals as required.

3.4 Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in IT / online safety/ health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided National Governors Association, other relevant organisation or as part of safeguarding training.
- Participation in school training / information sessions for staff or parents
- Bespoke training for governors provided by the school or other organisation.

A higher level of training will be made available to (at least) the Online Safety Governor. This will include Cyber-security training (at least at a basic level) and training to allow the governor to understand the school's filtering and monitoring provision.

4: Filtering & Monitoring

4.1 Filtering

The trust filtering and monitoring provision is agreed by the Trust Designated Safeguarding Lead, in conjunction with trustees, headteachers, Trust IT lead and the Trust IT Operations Manager and is annually reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. School DSLs are responsible for checking that the filtering system is working correctly at their school and for monitoring any breaches. Any issues giving rise to safeguarding or other safety concerns should be followed up as appropriate. The Trust IT team will support with technical queries and integration of the filtering system.

The trust manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering. Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.

Currently the Trust schools maintain and support the managed filtering service provided by the County ICT Service for pupils and staff in school. Schools have enhanced user-level filtering and tracking through the use of Smoothwall Monitor on all workstations, laptops and school provided devices, and may use other tools as required.

The Trust has different filtering levels for different ages and different groups of users: primary, secondary (11-16), post-16 and staff. School DSLs are able to ask for individual sites or pages to be removed from the filtered list (once they have checked they are suitable for the groups requested). They need to keep a log of all such sites/pages and the educational reason(s) for the request.

Where personal mobile devices (including phones) have internet access through the school network, access is limited to the lowest pupil-level filtering available in that school.

Any filtering issues should be reported immediately to the ICT Service/local IT Department.

All users have a responsibility to report immediately any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered, to the school IT support team for investigation. In addition, users must not attempt to use any programmes, software or other methods (such as online proxy sites) that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

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

Staff users will be made aware of the filtering systems through the AUP, induction training, and/or staff meetings, briefings, Inset as appropriate.

4.2 Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. For this reason, the Trust uses monitoring software (currently Smoothwall Monitoring).

The trust monitors all network users across all school-owned devices and services. All users are informed that the network (and devices) are monitored via the AUP agreements.

Monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead. Serious safeguarding alerts will be managed in line with safeguarding policy and practice.

Schools will have a protocol in place to report abuse/misuse. Any alerts that require rapid safeguarding intervention will be reported to the DSL immediately for action.

Staff can also directly monitor and control pupil use in lessons through real time software such as Apple Classrom (iPads) And NetSupport.

4.3 Oversight and Reporting

Filtering and monitoring logs are regularly reviewed by each school. Any issues are acted upon by the school DSL. Regular checks on the filtering system are undertaken by each school with any technical issues reported to the IT operations manager.

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

- The relevant governor or governors committee
- The trust DSL
- The school ISP or other external authorised body (including police) on request and as required.

5: Acceptable Use, Data Protection and Responding to Incidents

This policy and the acceptable use agreements define acceptable use at Trust schools. The acceptable use agreements will be communicated/re-enforced through communication with parents/carers, staff induction and handbook and through the school / trust websites.

5.1 Personal Data

The Cam Academy Trust aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

The Trust Data Protection policy, based on the data protection principles, applies to all personal data, regardless of whether it is in paper or electronic format. Staff must ensure that they are familiar with and comply with this policy. If staff have any questions about Data Protection, they should refer to this policy and/or the Trust Data Protection Officer (DPO).

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- 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.
- ensure that digital transmission of personal data is secure and encrypted and only to recognised and approved external bodies (e.g., exam boards and census returns)
- only transfer offline data using encryption and secure password protected devices.

Personal data should not be stored on any removable media (memory sticks, cards). If personal data is on a portable computer system:

- 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

When using any online storage system or data transfer system:

- the data must be encrypted and password protected
- only school approved systems should be used (OneDrive For Business); if in any doubt, confirm with IT department

Personal data must not be sent to personal email or cloud-based accounts.

5.2 Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using these technologies, the Trust consider the following as good practice:

- The official school digital communications may be regarded as safe and secure and are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g., by remote access or using cloud-based

services such as Microsoft Office 365).

- Users need to be aware that email communications may be monitored
- Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
- Users must report any email they consider to be a phishing email and must not respond to any such email.
- Any digital communication between staff and pupils or parents / carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social networking programmes must not be used for these communications.
- Pupils will be provided with individual school email addresses for educational use.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on school websites and only official email addresses should be used to identify members of staff.

5.3 Use of digital images and video

The development of digital imaging and video has created significant benefits to learning, allowing staff and pupils instant use of images, lesson recordings and live online sessions. However, staff and pupils need to be aware of the risks associated with sharing images and video, including publishing them on the internet. Images and video may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

Digital images

- The school may use live-streaming or video-conferencing services, most usually Microsoft Teams, in line with national and local safeguarding guidance / policies.
- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g., on social networking sites.
- Staff are allowed to take digital images to support educational aims, but must follow Trust policies concerning the sharing, distribution and publication of those images.
- Staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes
- If staff need to use personal equipment to record images, they must be uploaded to OneDrive within the Trust Microsoft Office 365 platform as soon as it is possible and any copies on their own device must be deleted.
- Care should be taken when taking digital images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Pupils must not store any images/video taken of others with their permission i.e., within lessons such as BTEC PE on any personal device. Any image/video taken on a personal device must be uploaded to OneDrive within the Trust Microsoft Office 365 platform.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are

able to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *learners* in the digital/video images

- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained via Data Checking Sheets before photographs of pupils are published on the school website/social media and information will be made available on revoking this permission.
- Parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- Images will be securely stored in line with the school retention policy

Video

- Staff are allowed to use video to support educational aims, but must follow Trust policies concerning the sharing, distribution and publication of those images.
- Staff must only communicate with pupils and parents / carers using official school systems or systems that have been approved by the Headteacher or senior leadership team.
- Staff must only communicate with pupils and parents / carers with the permission of Headteacher or senior leadership team e.g., during times of remote or hybrid learning, online parent consultation evenings or approved alternative provision.
- Staff must only record online meetings with permission of those involved and for a specific purpose e.g., went a member of staff is absent or unable to attend the meeting.
- If staff need to use personal equipment to record video, they must be uploaded to OneDrive within the Trust Microsoft Office 365 platform as soon as it is possible and any copies on their own device must be deleted.
- Pupils will not make or distribute, still images or recordings, video or audio of anyone involved **in any school activities**. This applies regardless of whether permission is given or not by the participant. There must be no recording of sound or video in any way.

5.4 Remote Learning

In addition to the points above, each school will have a policy or procedure on remote learning, setting out how the school will comply with the points above.

5.5 Social media

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through social media:

School staff should ensure that:

- no reference should be made in social media to learners, parents/carers or school staff.
- they do not engage in online discussion on personal matters relating to members of the school community.
- personal opinions should not be attributed to the school.
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

- they act as positive role models in their use of social media

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

- a process for approval by senior leaders
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts and an understanding of how incidents may be dealt with under school disciplinary procedures
- systems for reporting and dealing with abuse and misuse

Personal use

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school 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
- the school permits reasonable and appropriate access to personal social media sites during school hours

Parents

- when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this is not possible they will be encouraged to use the Trust complaints procedure.

5.6 Unsuitable / inappropriate activities

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

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
- promotion or conduct of illegal acts, e.g., under the child protection, obscenity, computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material in UK
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- promotion of any form of extremism or radicalisation
- threatening behaviour, including promotion of physical violence or mental harm
- 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

Users may not:

- use school systems to run a private business
- use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed the school
- upload, download or transmit commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- reveal or publicise confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords)
- create or propagate computer viruses or other harmful files
- carry out sustained or instantaneous high-volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- participate in on-line gaming (non-educational) or on-line gambling

5.7 Responding to incidents of misuse

It is hoped that all members of each school community will be responsible users of IT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

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

School policies and practice must ensure that:

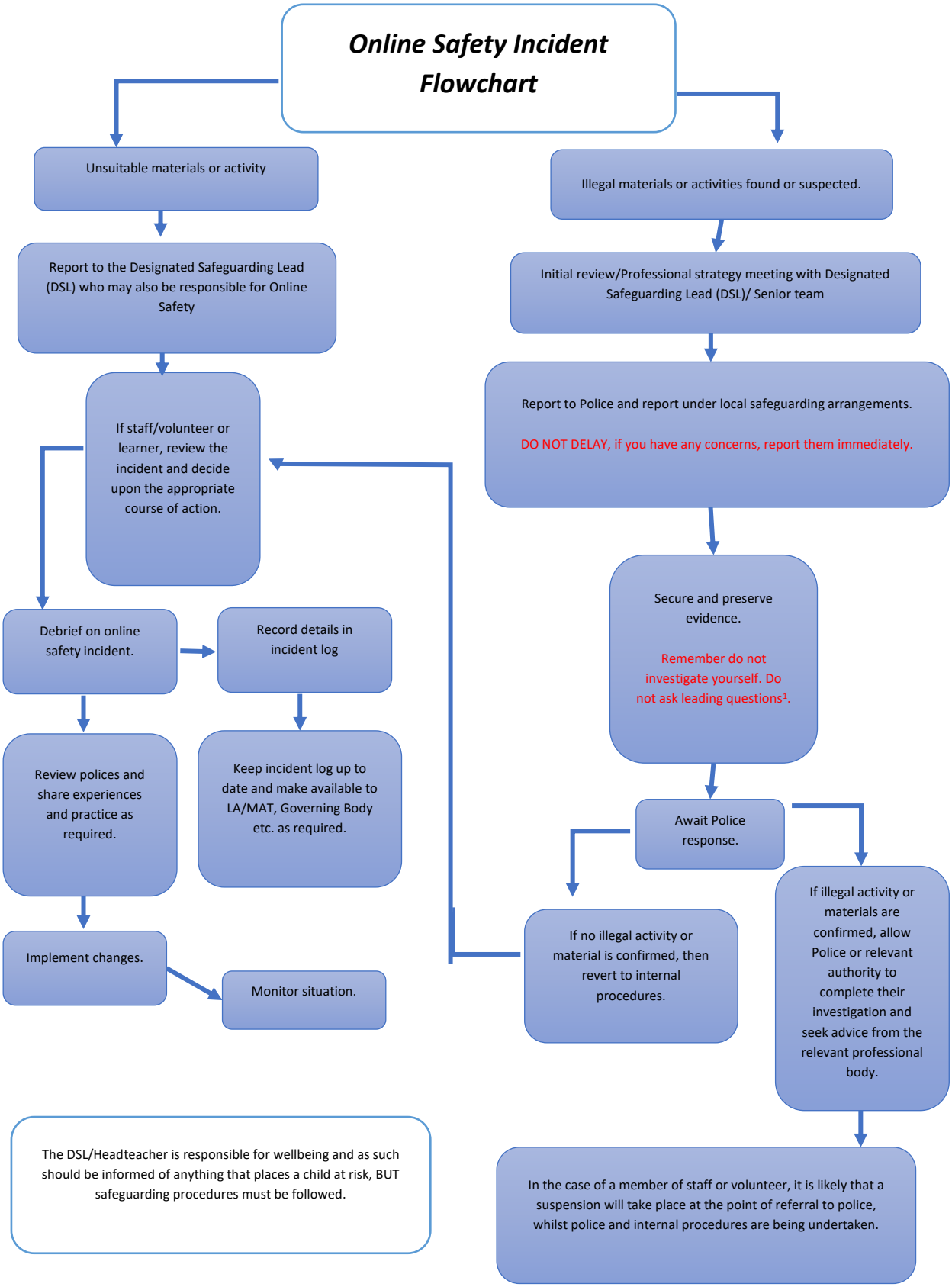
- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community are made aware of the need to report online safety issues/incidents
- those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- reports are dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm the incident must be escalated through the agreed school safeguarding procedures
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident

Any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Trust Chief Executive Officer. Where there is no suspected illegal activity, devices may be checked by the Headteacher / other DSL-trained member of the SLT in conjunction with IT support. They will 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. Investigating staff must be mindful that police may require this information if illegal activity were subsequently suspected.

Once the investigation has been completed, the Headteacher (or CEO) will need to judge what action, if any, should be taken.

Safeguarding incidents should be logged using My Concern and/or in line with school behaviour/disciplinary policies. Schools will seek to learn from any such incidents and use them to improve their practice.

The following flowchart summarises the process for an incident that is potentially illegal, or raises child protection concerns:


Online Safety Incident Flowchart
Unsuitable materials or activity
Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety
If staff/volunteer or learner, review the incident and decide upon the appropriate course of action.
Debrief on online safety incident.
Record details in incident log
Review polices and share experiences and practice as required.
Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.
Implement changes.
Monitor situation.
Illegal materials or activities found or suspected.
Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team
Report to Police and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not ask leading questions[1].
Await Police response.
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.
The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

Appendix A: The Cam Academy Trust IT Acceptable Use Policy - Staff

IT is an integral part of the way our schools work, and is a critical resource for pupils, staff, governors, volunteers and visitors. IT supports teaching and learning, pastoral and administrative functions within our schools.

This Acceptable Use Policy is intended to ensure:

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

The Trust will try to ensure that staff, governors and volunteers with each of its schools will have good access to IT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff, governors and volunteers to agree to be responsible users.

Definitions

"IT facilities": includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the IT service

"Users": anyone authorised by the school to use the IT facilities, including governors, staff, pupils and volunteers

"Personal use": any use or activity not directly related to the users' employment, study or purpose

"Materials": files and data created using the IT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

Acceptable Use Policy Agreement

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

System Security:

- I understand that the rules set out in this agreement also apply to use of school IT systems (e.g., any MIS, Office 365, the CATalogue etc.) out of school or working remotely.
- I understand that any device issued to staff (e.g., laptop, netbook, tablet etc.) is for the sole use of the member of staff it was issued to.
- I understand that I should not download programmes that have not been authorised by IT Support.
- I understand that I must not remove or attempt to inhibit any software placed on school devices that is required by the school for network compliance or security.
- I understand that I must not attempt to bypass any filtering and/or security systems put in place by the school.

- I understand that the school IT systems are primarily intended for educational use and that I will only use the systems for personal use within the policies and rules set down by this policy.
- I understand that the Trust accepts no liability for loss of any personal photographs, files or other information stored on school devices.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person.
- I will immediately report the receipt of any communication that makes me feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and will not respond to any such communication.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I understand that if I do not use synchronisation on my laptop, I am responsible for ensuring that my data is regularly backed up.
- I will not access, copy, remove or otherwise alter any other user's files without their express permission.
- I will take reasonable and appropriate steps to ensure that school provided equipment is looked after so as to avoid damage, loss or destruction
- I will report any damage or faults involving equipment or software, however this may have happened, as soon as I am able to.
- When I use my personal mobile devices (laptops / mobile phones / tablets / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses. *All breakages or loss of staff PMDs or the data therein are not the responsibility of the school or the Trust.*
- I understand that the school may monitor my use of the IT systems, email and other digital communications; this includes the use of any school device whilst away from school premises.
- I understand that the school may request the return of any equipment for any reason at any time by giving appropriate notice.
- I understand that if leave the employment of the school, I must return all IT equipment by the leaving date.

Data Protection

- I am aware of my responsibilities under Data Protection legislation (including GDPR) regarding personal data of pupils, staff or parents/carers.
- I understand I should use designated school software such as SIMS, Bromcom, Go4Schools or other proprietary software to view personal pupil information, wherever possible to ensure security of information.
- I am aware that all data and communications (including but not limited to emails, chats and files) created or received as part of my school role may be subject to disclosure in response to a request for information under the Freedom of Information Act 2000 or a Subject Access Request under the Data Protection Act 2018.
- I will ensure that all communications, especially regarding pupils, are appropriate and of a professional nature.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. If I need to use my personal equipment to record these images, I will download them to the school network as soon as

is possible and delete any copies on my own device. Where these images are published it will not be possible to identify by name, or other personal information, those who are featured.

- I will only transport, hold, disclose or share personal information about others, or myself as outlined in the relevant Trust policies. Where personal or sensitive data is transferred outside the secure school network or Office 365 (e.g., on USB devices), it must be encrypted.
- I will only use the Trust provided secure cloud storage facilities, Microsoft OneDrive for Business and SharePoint/the CATalogue. I understand that all other cloud storage solutions are not to be used.
- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download, share or distribute copies (including music and videos).

Safeguarding:

- I understand that I am expected to immediately report any illegal, inappropriate or harmful material or incidents I become aware of, to the Designated Safeguarding Lead.
- I am aware that any queries or questions regarding safe and professional practice online either in school or off site should be raised with the Designated Safeguarding Lead or the Head teacher.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not knowingly use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will only use social networking sites in school in accordance with the school's policies/guidance.
- When communicating with pupils and parents / carers, or in any other professional capacity, I will only use official school systems, email accounts etc. I will not use personal e-mail addresses, text messaging or social media accounts. Any such communication will be professional in tone and content.
- I will follow good practice when using personal social media regarding my own professional reputation and that of the school and its community and will not engage in any on-line activity that may compromise my professional responsibilities.

Remote Online Working:

I understand that if I am delivering learning remotely:

- I must not have 1:1 audio or video meetings with pupils unless they have been approved with the Headteacher and an appropriate safeguarding risk assessment has taken place and is documented.
- I understand that any lesson resources that are recorded by a member of staff should be audio and not video i.e., a Loom or Screencast -O-Matic recording, unless this has been approved by the Headteacher or designated member of the senior leadership team.
- I must only communicate with pupils and parents / carers using official school systems or systems that have been approved by the Headteacher or senior leadership team.
- I must not use personal emails or non-school sanctioned social media to carry out any contact with pupils and parents.
- I understand that any use of personal phones to contact parents or pupils must be part of a school-sanctioned initiative and I must use 141 to withhold the number, unless approved with the Head teacher and an appropriate safeguarding risk assessment has taken place and is documented.
- I understand that all communication will be professional in tone and manner.
- I should use school devices over personal devices wherever possible. If using personal devices, please use Trust approved web-based IT systems such as Office 365 or the CATalogue. Please ensure

that personal details, such as usernames and passwords, are not saved on logon pages such as email, Go for Schools or Office 365.

- I must not engage in any on-line activity that may compromise their professional responsibilities or cause embarrassment to the school or the Trust.
- I understand that all staff communications should be within school hours as much as possible (or hours agreed with the school to suit the needs of staff).
- I will not use systems outside of Trust approved IT environment, without seeking approval from the Head teacher and Trust Director of IT Strategy and an appropriate safeguarding risk assessment has taken place and is documented.
- If attending online meetings with colleagues or delivering online learning I must:
    - Behave in a professional manner,
    - Dress appropriately,
    - Be in an appropriate space for the meeting or blur backgrounds,
    - Try to avoid interruptions etc.
- When planning online activities, I will consider carefully
    - Pupil access to IT and internet,
    - Home internet content filtering systems,
    - Bandwidth demands of the work being set,
    - Costs that may be incurred by parents/carers when pupils are accessing work, i.e., video streaming or downloading resources,
- I will report any behavioural incidents according to the guidelines set out in the school behaviour policy.
- I will report any safeguarding incidents or potential concerns according to the guidelines set out in the school safeguarding policy.

Staff Agreement

I understand that I am responsible for my actions in and out of school:
• I understand that this Acceptable Use Policy applies not only to my work and use of school IT equipment in school, but also to my use of school IT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
• I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities, the involvement of the police.

I have read and understand the policy and agree to follow these guidelines when:
• I use the school IT systems and equipment (both in and out of school)
• I use my own equipment in school
• I use my own equipment out of school in a way that is related to me being a member of this school e.g., communicating with other members of the school community, accessing school email or online resources, theCATalogue, etc.

Name of Member of Staff **Position/ Dept.**

Signed **Date**

Appendix B: The Cam Academy Trust IT Acceptable Use Policy – Pupils

The Cam Academy Trust recognises the essential and important contribution that technology plays in promoting learning and development, both at school and at home. We believe that by fully embracing technology in the education process we can help our pupils to:

- Learn powerfully
- Learn for life
- Learn from one another

The Cam Academy Trust seeks to ensure that all members of our community are safe and responsible users of technology. We will support our pupils to:

- Become empowered and responsible digital creators and users
- Use our resources and technology safely, carefully and responsibly, respecting system security and password security
- Be kind online and help us to create a community that is respectful and caring, on and offline
- Be safe and sensible online, and always know that all pupils can talk to a trusted adult if they are unsure or need help.

All pupils within our Trust have the opportunity to use a range of IT resources, including internet access, as an essential part of learning. This includes access to:

- Computers, laptops and other digital devices such as iPads
- The internet, which may include search engines and educational sites
- School learning platforms such as the CATalogue
- Email
- Digital cameras, webcams and video cameras

This policy sets out our expectations of pupils and how they use and interact with IT systems in our schools. Pupils should be made aware of these expectations in an age-appropriate way. In the case of Key Stage 3-5 pupils, they should be given a copy of the following and confirm their understanding by signing the Key Stage 3-5 agreement. Key Stage 2 and 1 pupils should sign the amended agreements that follow.

ICT Acceptable Use Agreement – Secondary Pupils

General Expectations

- Pupils (and their parents/carers if working remotely) will be expected to take responsibility for the use of all IT related to schoolwork, making sure that the technology is used safely, responsibly and legally.
- Pupils (and their parents/carers if working remotely) will be expected to take personal responsibility for their own e-safety. Advice and resources can be found on individual school websites.
- Pupils must not give out any personal details or arrange to meet someone online without the written permission of a parent, carer or teacher.
- Pupils must report anything that makes them feel uncomfortable or unhappy to a teacher or trusted adult.
- Pupils must not make or distribute, still images or recordings, video or audio of anyone involved **in any school activities**. This applies regardless of whether permission is given or not by the participant. There must be no recording of sound, video or image, in any way.
- Pupils must use email responsibly and always be polite and respectful.
- For schoolwork pupils must only use email or other messaging methods that are provided by the CAM Academy Trust.
- IT systems must not be used for bullying or harassing others or in a way that will bring the school into disrepute.
- Pupils must not download or install any software or files on the school's IT equipment (unless it is a requirement of an agreed course of study) or open emails or attachments from people that they do not know.
- USB drive (memory stick) that are used in school to store or transfer files must have been virus checked first.
- Pupils must not intentionally gain access to unsuitable or illegal sites nor try to use any programs that allow them to bypass any filtering/security systems.
- Pupils must not access any video broadcasting or social media sites unless given permission to do so. Any accidental access to such sites must be reported as soon as possible.
- Pupils must only access the school computer systems (network, Internet, email and the CATalogue where provided) using their own login and password, which must keep secret.
- Pupils must ensure that their work does not break The Copyright, Design and Patents Act. The source of information (words, images etc.) must be acknowledged.
- Pupils must not use the school IT systems to copy other people's work and pass it off as my own (plagiarism).
- Pupils must use school ICT equipment with care and report any damage which occurs as soon as possible.
- Personal mobile devices (mobile phones / iPads etc.) should only be used in school if permission has been given and follow the school's personal mobile phone policy.
- Pupils must use network resources responsibly
    - think and then preview before I print
    - regularly review my files and delete them when no longer needed
    - only store school-related files and images on the school network
    - only use the ICT equipment for school related work unless I have permission from an appropriate member of staff

Remote Working Expectations

- Pupils working remotely should continue to follow the expectations contained within the relevant behaviour policies of their school
- Pupils should only attend online teaching sessions to which they've been directly invited by a member of staff.
- If attending an online teaching session, pupils must ensure that their video facility is off before entering the session.
- If attending an online teaching session, pupils must behave appropriately and respect the teacher and other pupils who may be attending.
- Pupils will not make or distribute, still images or recordings, video or audio of anyone involved **in any school activities**. This applies regardless of whether permission is given or not by the participant. There must be no recording of sound, video or image, in any way
- Pupils may be asked by their school to upload a specific image, video or audio relating directly to their home learning that provides evidence of knowledge and understanding. In some schools this may be required to be agreed by the school and parent.
- Pupils should only upload images or videos to a specific location as directed by a member of staff.

Pupils should understand that the school also has the right to take action against them if they are involved in incidents that contravene this policy or other school policies relating to acceptable pupil behaviour, when they are out of school or where they are involved with any member of the school community (examples would be cyber-bullying, use of images or personal information).

Pupil Acceptable Use Agreement Form - Key Stage 3-5

Please complete the sections below to show that you have read, understood and agree to the expectations outlined above in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school IT systems and equipment (both in and out of college)
- I use my own equipment in school (when allowed) e.g., mobile phones, PDAs, cameras etc.
- I use my own equipment out of college in a way that is related to me being a member of this school e.g., remote learning, communicating with other members of the school, accessing school email, the CATalogue, etc.

Name of Pupil

Signed **Date**

Cam Academy Trust IT Acceptable Use Agreement – Key Stage 2

- I will use the school's ICT equipment and tools for schoolwork and homework. If I need to use the school's computers for anything else, I will ask for permission first.
- I will only use the Internet if a teacher or teaching assistant is in the room with me.
- I will only delete my own files unless my teacher gives me permission to delete someone else's. I will not look at other people's files without their permission.
- I will keep my passwords private and tell an adult if I think someone else knows them. I know that my teacher can change my Purple Mash, Sum Dog or Times Table Rockstars passwords if needed.
- I will only open e-mail attachments from people who I know or an adult has approved. If I am unsure about an attachment or e-mail, I will ask an adult for help.
- I will not give my own personal details such as surname, phone number or home address or any other personal details that could be used to identify me, my friends or my family. If I have to use an online name I will make one up!
- I will never post photographs or video clips of people I know without permission and never include names with photographs or videos.
- I will never arrange to meet someone I have only ever previously met online. It could be dangerous.
- I will not deliberately look for, save or send anything that could be unpleasant or upsetting. If I find anything via Internet, e-mail or mobile phone that is upsetting or makes me feel uncomfortable, I will tell a teacher or responsible adult.

I will do my best to follow these rules because I know they are there to keep me and my friends safe. If I don't follow these rules, my teacher may:

- Speak to me about my behaviour.
- Speak to my parents about my use of technology.
- Remove me from online communities or groups.
- Turn off my access for a little while.
- Not allow me access to use laptops / computers to access the internet or particular programmes.
- Take other action to keep me (and others) safe.

I am signing below to show that I understand and will try to abide by these rules

Name: Date:

Signature:

Cam Academy Trust IT Acceptable Use Agreement – Key Stage 1

This is how we stay safe when we use computers:

- I will only use the school's computers or iPads when I am told to by a teacher or suitable adult or when I have asked them for permission first.
- I will only use school computers and iPads for schoolwork and homework. If I need to use the school's computers for anything else, I will ask first.
- I will only use the internet and email when an adult is nearby.
- I will not share my passwords with other people and will tell my teacher if I think someone else knows them.
- I will ask an adult before opening an email from someone I don't know.
- I will not share details about myself such as surname, phone number or home address.
- I will ask if I need to look at other peoples' work on the computer.
- I will try my hardest to only send messages which don't upset other people.
- I will ask my teacher before using photos or video.
- If I see something on a screen which upsets me, I will always tell an adult.

I will do my best to follow these rules because I know they are there to keep me and my friends safe. If I don't follow these rules, I know that my teacher may stop me using technology at school and talk to my parents.

Pupil's name:

Pupil's signature:

Date:

Appendix C: The Cam Academy Trust IT Acceptable Use Policy – Community Tutors

This Acceptable Use Policy is intended to ensure that

- Community tutors will be responsible users and stay safe while using the internet and other technologies within their educational role at Cam Academy Trust schools.
- The Trust's IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Policy Agreement

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

System Security:

- I understand that the rules set out in this agreement also apply to use of school IT systems (e.g., any MIS, Office 365, the CATalogue etc.) out of school or working remotely.
- I understand that I should not download programmes that have not been authorised by IT Support.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I understand that I must not remove or attempt to inhibit any software placed on school devices that is required by the school for network compliance or security.
- I understand that I must not attempt to bypass any filtering and/or security systems put in place by the school.
- I understand that the school IT systems are intended for educational use and that I will not use the systems for personal use.
- I understand that the Trust accepts no liability for loss of any personal files or other information stored on school devices.
- I will not disclose my username or password to anyone else.
- I will not access, copy, remove or otherwise alter any other user's files without their express permission.
- I will take reasonable and appropriate steps to ensure that school provided equipment is looked after so as to avoid damage, loss or destruction
- I will report any damage or faults involving equipment or software, however this may have happened, as soon as I am able to.
- When I use my personal mobile devices (laptops / mobile phones / tablets / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses. *All breakages or loss of staff PMDs or the data therein are not the responsibility of the school or the Trust.*
- I understand that the school will monitor my use of the IT systems and network.

Data Protection

- I am aware of my responsibilities under Data Protection legislation (including GDPR) regarding personal data of those I teach.
- I am aware that all data and communications (including but not limited to emails, chats and files) created or received as part of my community role may be subject to disclosure in response to a

request for information under the Freedom of Information Act 2000 or a Subject Access Request under the Data Protection Act 2018.

- I will ensure that all communications are appropriate and of a professional nature.
- I will not make or distribute, still images or recordings, video or audio of anyone involved in any community learning activities, unless expressly required for a specific qualification. In this case, they will be kept secure and in line with GDPR requirements, and will be deleted as soon as they are no longer required.
- I will only transport, hold, disclose or share personal information about others, or myself as outlined in the relevant Trust policies.
- I will only use the Trust provided secure cloud storage facilities, Microsoft OneDrive for Business and SharePoint/the CATalogue. I understand that all other cloud storage solutions are not to be used.
- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download, share or distribute copies (including music and videos).

Safeguarding:

- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person.
- I will immediately report the receipt of any communication that makes me feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and will not respond to any such communication.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- When communicating with learners I will only use official school systems, email accounts etc. I will not use personal e-mail addresses, text messaging or social media accounts. Any such communication will be professional in tone and content.
- I will follow good practice when using personal social media regarding my own professional reputation and that of the school and its community and will not engage in any on-line activity that may compromise my professional responsibilities.

Staff Agreement

• I understand that this Acceptable Use Policy applies not only to my work and use of school IT equipment in school, but also to my use of personal equipment in school or in situations related to my employment by the school.
• I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, termination of contract and, in the event of illegal activities, the involvement of the police.

I have read and understand the policy and agree to follow these guidelines when:
• I use the school IT systems and equipment
• I use my own equipment in school
• I use my own equipment out of school in a way that is related to me being a tutor at this school.

Name of Tutor

Signed **Date**

Appendix D: Personal Mobile Devices (PMDs)

Personal Mobile Devices (PMD) include mobile phones, smart watches, tablets, iPods, MP3 players, and games consoles. Any device that is part of a school-based 1:1 scheme will be covered by this framework, but not classified as a personal device as it is owned by the school until the lease has finished.

The Cam Academy Trust recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within our schools. Whilst any PMD connected to a school network will have the highest level of filtering available, school systems cannot monitor or control content accessed over phone networks. It is also not possible to identify individual users of PMDs on school networks and so the usual levels of traceability do not apply.

It is therefore extremely important that each Trust school should have clear expectations and processes in place to deal with the use of personal mobile devices. This may be in the form of a distinct policy but alternatively may be contained within other documentation, eg behaviour policies, codes of conduct etc.

These expectations and processes must:

- Be developed in accordance with the law and other appropriate policies such as Pupil Discipline and Behaviour, Safeguarding and Child Protection and Pupil Acceptable use of IT, Remote Online Working Guidelines and Guidelines for Attending Live Sessions.
- Explain how pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and how they will be made aware of boundaries and consequences.
- State that the school accepts no responsibility for replacing lost, stolen or damaged mobile phones and accepts no responsibility for pupils who lose or have their PMDs stolen while travelling to and from school.
- Be clear about the expectations regarding PMD usage within school time. In particular, that PMDs must not be used within school to record, take or share images, video and audio of other pupils or staff (unless using school devices, which includes devices that is part of a school-based 1:1 scheme, for educational purposes).
- Explain arrangements for parent – pupil contact/communication during school hours which negate the need to use a PMD in these circumstances.
- Explain any differences in expectations / rules which may apply during school visits, trips, including overseas, residential etc – or clarify that this will be explained as part of the information for each trip where it differs from normal in-school expectations.
- Explain how the school will deal with the discovery of any inappropriate/undesirable imagery or material, including that which promotes pornography, violence or bullying of any description or which may be offensive, derogatory or otherwise contravene other relevant school policies, eg Behaviour, Anti-Bullying, Safeguarding and Child Protection and Acceptable use of IT.
- Explain how the school will deal with the sending of abusive or inappropriate messages or content, both inside and outside school (or refer to another policy where this is covered).
- Explain the processes for confiscating devices, including those for returning, and how, if there is suspicion of illegal or criminal activity, a device may be handed over to the police for further investigation.