THE

NEW GUILD

TRUST

Online Safety Policy

POLICY

This policy has been adopted on behalf of all academy schools within The New Guild Trust:

Moorpark Junior School
Jackfield Infant School
Alexandra Junior School
Alexandra Infants' School

Approval and Review

Committee to Approve Policy	Trust Board
Date of Trustee Board / Academy Committee Approval	February 2025
Chair of Trustee Board / Academy Committee	Mrs L Eagle
Signature	*L Eagle*
Accounting Officer	Mrs K Peters
Signature	*K Peters*
Policy Review Period	12 months
Date of Policy Review	February 2026

Version Control

Version	Date Approved	Changes	Reason for Alterations
Initial	May 2019		Initial version for Moorpark Junior School
2	Nov 2020	P4: It has been reviewed by the Executive Board.	Review, not initial development
3	Nov 2021	P4 schedule for review replaced by p2: approval and review	Redundant schedule
		P5 deleted name "E Searl"	To make policy generic
		P6 deleted name "E Searl"	To make policy generic
		P7 added "or CoRE" and deleted name "E Searl"	To make policy generic
		P12 added "or CoRE"	To make policy generic
4	Jan 2023	P3 "inline" to "online"	Correct typo
		P3 added "each"	To make generic
		P3 added "and Trustees"	To reflect that this is a Trust wide matter and to follow newest guidance
		P3 added passage outlining Governors/ Trustees role P4 added "Designated Safeguarding Lead" P4 rewrote first paragraph under the Headteacher heading	To reflect new guidance (KCSIE 22)

		P4, P8 deleted “EVOLVE”	No longer a technical support provider

Version Control (cont’d)			
Version	**Date Approved**	**Changes**	**Reason for Alterations**
		P4 deleted “leads the Online Safety Group” P5 deleted paragraph about Online Safety Group	No longer active
		P7 added Governors/Trustees will receive online safety information and training on induction	To reflect new guidance (KCSIE 22)
		P7 changed “Directors” to “Trustees”	
		P16 added “Recent Guidance” The policy has been reviewed following the latest guidance in KCSIE 2022	To acknowledge latest guidance
5	Mar 2024	P3 edited wording of “DSLs understand their responsibility in understanding the appropriate filtering and monitoring systems and processes in school”	To reflect new guidance (KCSIE 23)
		P4 added “It is part of the DSL’s responsibilities to take a lead on understanding the filtering and monitoring systems and processes in school.”	To reflect new guidance (KCSIE 23)
		P5 added “including filtering and monitoring systems in school.”	To reflect new guidance (KCSIE 23)
		P6-P9 added a lot of detail to section on **Education pupils**	To add more detail to this section that reflects new guidance on teaching on line safety in schools (updated in January 2023)
		P11 rewritten “The school uses a monitoring system that captures, records and reports any suspicious or inappropriate activities”	School staff no longer do this but a company that reports to school staff
6	October 2024	P3 added paragraph of the purpose of the policy as this was missing	Used newest NSPCC guidance (Feb 22)

Development/Monitoring/Review of this Policy

This Online Safety Policy has been developed by the Personal Development and Welfare Committee made up of:

- Headteacher/Senior Leaders
- Online Safety Officer/Coordinator
- Staff – including Teachers, Support Staff, Technical staff
- Local Community Governors/Trust Board

Consultation with the whole school community has taken place through a range of formal and informal meetings.

It has been reviewed by the Executive Board.

The school will monitor the impact of the policy using:
- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) • Internal monitoring data for network activity
- Surveys / questionnaires of:
  - pupils
  - parents/carers
  - staff

Purpose of this policy

The updated definition of safeguarding (in line with the updated 'Working Together to Safeguarding Children' guidance) now explicitly includes recognition that children may be maltreated online.

The purpose of this policy statement is to:

• ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
• provide staff and volunteers with the overarching principles that guide our approach to online safety
• ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

Scope of the Policy

This 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 computer systems, both in and out of the school.

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 school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. 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 published Behaviour and Rewards Policy.

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

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within each school:

Governors and Trustees:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. Governors/Trustees ensure that the DSLs understand their responsibility in understanding the appropriate filtering and monitoring systems and processes in school, manage them effectively and know how to escalate concerns when identified. Reviews will be carried out by the Local Community Governors/Committee receiving regular information about online safety incidents and monitoring reports. A member of the Local Community Governing Body/Trust Board has taken on the role of Online Governor.

The role of the Online Governor will include:

- Regular meetings with the Online Safety Co-ordinator/Officer
- Regular monitoring of online safety incident logs – reported Termly
- Regular monitoring of filtering/change control logs
- Reporting to relevant Governor committee/meeting

Headteacher, Designated Safeguarding Lead and Senior Leaders:

- Online safety is part of our statutory safeguarding responsibilities – in our schools safeguarding is everybody's responsibility. The Headteacher/Designated Safeguarding Lead have overall responsibility for online safety and they access appropriate training and support to enable them to keep up to date. It is part of the DSL's responsibilities to take a lead on understanding the filtering and monitoring systems and processes in school.
- The day to day responsibility for online safety will be delegated to the Online Safety Coordinator/Officer.
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR/other relevant body disciplinary procedures).
- The Headteacher/Senior Leaders are responsible for ensuring that the Online Safety Coordinator/Officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Coordinator/Officer.

Online Safety Coordinator/Officer:

- Takes day to day responsibility for online issues and has a leading role in establishing and reviewing the school e-safety policies/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff.
- Liaises with the Local Authority/relevant body.
- Liaises with school technical staff.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Meets regularly with the Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs.
- Attends relevant meeting/committee of Governors.
- Reports regularly to the Senior Leadership Team.

Network Manager/Technical staff:

The Technical Staff – CoRE Computing are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required e-safety technical requirements and any Local Authority/other relevant body Online Safety Policy/Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- The filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.

- That the use of the network/internet/Virtual Learning Environment/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/Senior Leader; Online Safety Coordinator /Officer for investigation/action/sanction.
- That monitoring software/systems are implemented and updated as agreed in school policies.

Teaching and Support Staff:

The teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online policy and practices including filtering and monitoring systems in school.
- They have read, understood and signed the Staff Acceptable Use Policy/Agreement (AUP)
- They report any suspected misuse or problem to the Headteacher /Senior Leader/Online Safety Coordinator/Officer for investigation/action/sanction.
- All digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems
- Online Safety issues are embedded in all aspects of the curriculum and other activities. Every half term teachers will plan online safety awareness sessions into their lessons and embed the online safety rules.
- Pupils understand and follow the e-safety and acceptable use policies.
- 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 (see Mobile Phone Protocol Policy).
- In lessons where internet use is pre-planned 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.

Child Protection/Safeguarding Designated Person/Officer:

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

Pupils:

- Are responsible for using the *school's* digital technology systems in accordance with the Pupil Acceptable Use Policy.
- 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 policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying.
- Should understand the importance of adopting good e-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.

Parents/Carers:

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

- Digital and video images taken at school events.
- Access to parents' sections of the website / VLE and on-line pupil records.
- Their children's personal devices in the school (where this is allowed).

Community Users:

Community Users who access school systems/website/VLE as part of the wider school provision will be expected to sign a Community User AUP before being provided with access to school 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. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Schools follow the newest advice "Teaching Online Safety in Schools" (updated 12.01.2023
As part of the statutory relationships and health education, pupils are taught about online safety and harms. This includes being taught:

- What positive, healthy and respectful online relationships look like.
- The effects of their online actions on others.
- How to recognise and display respectful behaviour online.

This complements the computing curriculum, which covers the principles of online safety in all year groups, with progression in the content to reflect the different and escalating risks that pupils face. This includes:

- How to use technology safely, responsibly, respectfully and securely
- Where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Key online safety messages are also reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information. They are taught to consider:
  - whether a website, URL or email is fake
  - what cookies do and what information they are sharing
  - if a person or organisation is who they say they are
  - why a person wants them to see, send or believe something
  - why a person wants their personal information
  - the reason why something has been posted
  - whether something they see online is fact or opinion

Pupils will be enabled to recognise the techniques that are often used to persuade or manipulate others. Pupils are taught to recognise:

- Online content which tries to make people believe something false is true or mislead (misinformation and disinformation)
  Techniques that companies use to persuade people to buy something
- Ways in which criminals may try to defraud people online
- Ways in which games and social media companies try to keep users online longer (persuasive or sticky design)
- Grooming and manipulation techniques used by criminals
- Ways to protect themselves from a range of cyber crimes

We want pupils to understand what acceptable and unacceptable online behaviour look like. We teach pupils:

- That the same standard of behaviour and honesty apply on and offline, including the importance of respect for others
- To recognise unacceptable behaviour in others by:
  - looking at why people behave differently online, for example how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do
  - Looking at how online emotions can be intensified resulting in mob mentality[footnote 1]
  - Looking at the key principles behind a constructive discussion, including a willingness to listen to other opinions and a readiness to be educated on a topic
  - Considering how to demonstrate empathy towards others (on and offline)
  - Teaching techniques (relevant on and offline) to defuse or calm arguments, for example, a disagreement with friends, and disengage from unwanted contact or content online
  - Considering unacceptable online behaviours often passed off as so-called social norms or just banter, for example, negative language being used as part of online gaming but would never be tolerated offline.

Pupils will be taught to identify and manage risk by discussing:
- The ways in which someone may put themselves at risk online
- Risks posed by another person's online behaviour
- When risk taking can be positive and negative
- Age-restrictions and what they are for
- Online reputation and the positive and negative aspects of an online digital footprint
- Sharing information online and how to make a judgement about when and how to share and who to share with.
- The risks of cyber crime, online fraud and identity theft.

Pupils are taught how and when to seek support. We explain how to:
- Identify who trusted adults are.
- Access support from the school, police, the National Crime Agency's Click CEOP reporting service for children and 3rd sector organisations such as Childline and Internet Watch Foundation.
- Report cyber crime, fraud and suspicious online activity, through organisations such as Action Fraud and the Advertising Standards Authority.
- Report inappropriate contact or content for various platforms and apps.

The internet and social media make spreading divisive and hateful narratives easier. Extremist and terrorist groups and organisations use social media (for example, apps, forums, blogs, chat rooms) to identify and target vulnerable individuals. To fulfil our responsibilities under the PREVENT duty we teach:
- How to recognise extremist behaviour and content online
- Understanding actions which could be identified as criminal activity
- Exploring techniques used for persuasion
- Knowing how to access support from trusted individuals and organisations
- To protect our pupils well being we teach about:
- Self-image and identity
- Online reputation
- Online bullying
- Health, wellbeing and lifestyle

We include:
- Helping pupils to evaluate critically what they are doing online, why they are doing it, and for how long (screen time).
- Helping pupils to consider quality versus quantity of online activity.
- Explaining that pupils need to consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or the fear of missing out.

- Helping pupils to understand that time spent online gives users less time to do other activities - this can lead to some users becoming physically inactive.
- Exploring the impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues.
- Explaining that isolation and loneliness can affect pupils and that it is very important for pupils to discuss their feeling with an adult and seek support.
- Where to get help.

Other teaching points include:
- 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 helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices.
- In lessons where internet use is pre-planned, 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, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Vulnerable Pupils

Any pupil can be vulnerable online, and their vulnerability can fluctuate depending on their age, developmental stage and personal circumstance.

However, there are some pupils, for example, looked after children and those with special educational needs, who may be more susceptible to online harm or have less support from family or friends in staying safe online. Teachers consider how to tailor our offer to make sure these pupils receive the information and support they need.

Safeguarding

As with any safeguarding lessons or activities, it is important to consider the topic they are covering and the potential that a child (or more than one child) in the class may be suffering from online abuse or harm in this way.

It is important to create a safe environment in which pupils feel comfortable to say what they feel. If a pupil thinks they will get into trouble or be judged for talking about something which happened to them online they may be put off reporting it and getting help.

Where we are already aware of a child who is being abused or harmed online we carefully plan any lesson to consider this, including not drawing attention to that child in a way that would highlight or publicise the abuse. It is good practice to include the designated safeguarding lead (or a deputy) when planning any safeguarding related lessons or activities (including online). They will be best placed to reflect and advise on any known safeguarding cases, and how to support any pupils who may be especially impacted by a lesson.

In some cases, a pupil will want to make a disclosure following a lesson or activity. The lesson may have provided the knowledge that enabled the pupils to realise they are being abused or harmed or give them

the confidence to say something. This is why it is essential all pupils are clear what the school's reporting mechanisms are.

Education – Parents/Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's 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.

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

- Curriculum activities.
- Letters, newsletters, web site, VLE.
- Parents/Carers evenings/sessions.
- High profile events/campaigns e.g. Safer Internet Day.
- Reference to the relevant web sites/publications.

Education – The Wider Community

The school will provide opportunities for local community groups/members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety.
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The academy school website will provide online information for the wider community.

Education & Training – Staff/Volunteers

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

- A planned programme of formal online safety training will be made available to staff.
- This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly. It is expected that some staff will identify online safety as a training need within the performance management process.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- The Online Safety Coordinator/Officer (or other nominated person) will receive regular updates through attendance at external training events (e.g. from SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in team meetings/INSET days.
- The Online Safety Coordinator/Officer (or other nominated person) will provide advice/ guidance/training to individuals as required.

Training – Governors/Trustees

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

- Attendance at training provided by the Local Authority/National Governors.
- Association/or other relevant organisation (e.g. SWGfL).
- Participation in school training/information sessions for staff or parents.

Technical – Infrastructure /Equipment, Filtering and Monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school academy technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted. All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by CoRE who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every 30 days.
- The "master/administrator" passwords for the school/academy IT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. School Safe).
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. 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.
- The school uses a monitoring system that captures, records and reports any suspicious or inappropriate activities of users on the school technical systems to the DSL. Users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).
- 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 virus software.
- An agreed policy is in place regarding the extent of personal use that users (staff/pupils).
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed Personal Data Policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

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. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for 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. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the GDPR). 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 pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

General Data Protection Regulations (GDPR)

Personal data will be recorded, processed, transferred and made available according to the GDPR regulations 2018, 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.

The school must ensure 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".
- It has a GDPR Policy.
- It is registered as a Data Controller for the purposes of the GDPR.
- 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 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, in line with school policy (below) 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. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

Communication Technologies	Allowed	Allowed at Certain Times	Allowed for Selected Staff	Not Allowed	Allowed	Allowed at Certain Times	Allowed with Staff Permission	Not Allowed
Mobile phones may be brought to school	X							X
Use of mobile phones in lessons				X				X
Use of mobile phones in social time	X							X
Taking photos on mobile phones or other camera devices		X					X	
Use of hand held devices, e.g. PDAs, PSPs		X					X	
Use of personal email addresses in school, or on school network				X				X
Use of school email for personal emails		X						X
Use of chat rooms/facilities				X				X
Use of instant messaging		X						X
Use of social networking sites				X				X
Use of blogs		X					X	

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school academy systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email, chat, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities 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 academy school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

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

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable /Inappropriate Activities

The school 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 usage as follows:

User Action		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	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	
comments that contain or relate to:	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				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 school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. 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	

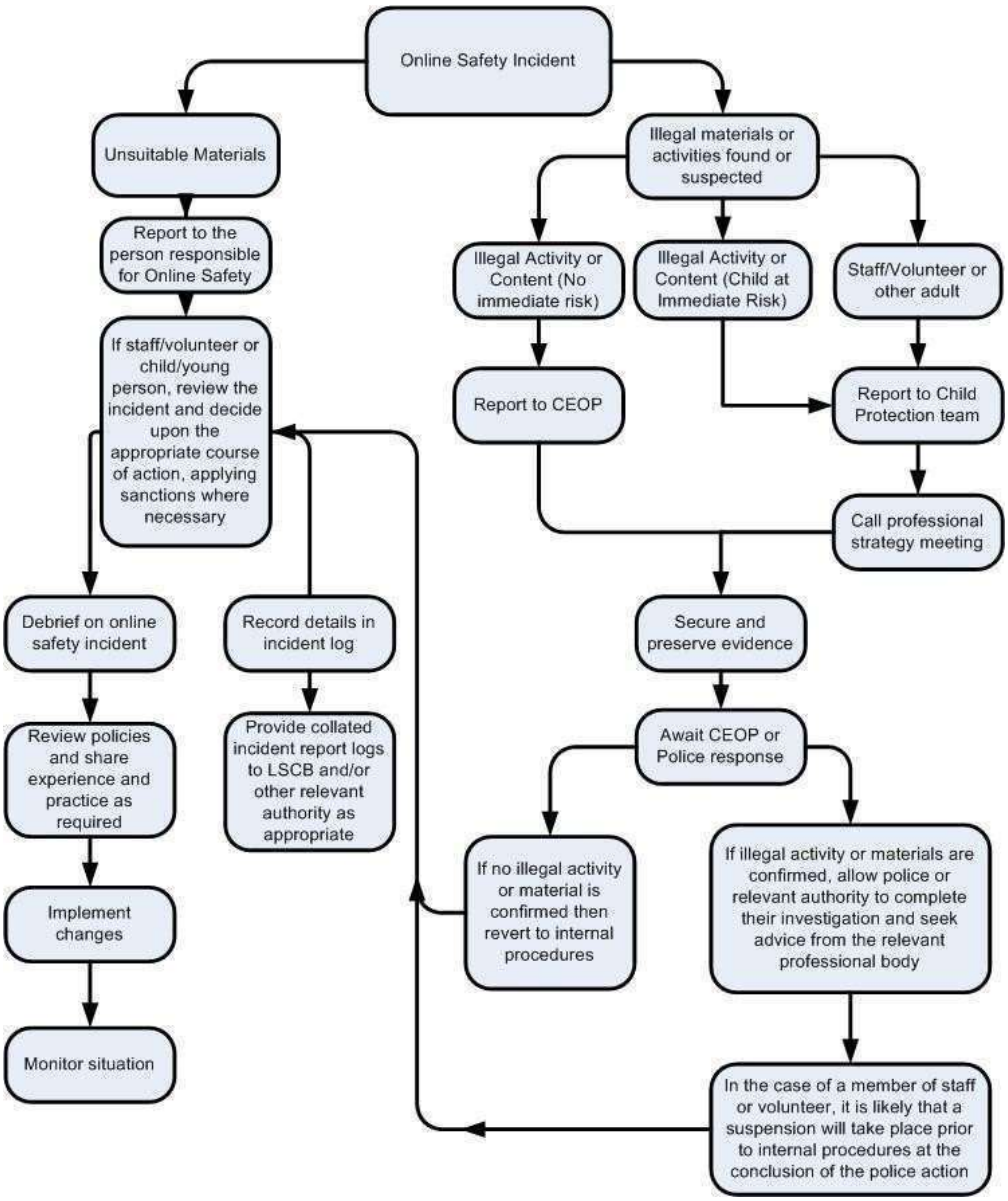
Use of video broadcasting e.g. Youtube		X			

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 for responding to online safety incidents and report immediately to the Police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow academy school 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/volunteer 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 the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority 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
  - 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 the school and possibly the Police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

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

Pupil Actions / Sanctions

Incidents:	Refer to class teacher	Refer to Head of Department / Head of Year / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering/security etc	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanction e.g. detention/ 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	X	X
Unauthorised use of non-educational sites during lessons	X		X			X		X	X
Unauthorised use of mobile phone/digital camera/other handheld device	X		X			X		X	X
Unauthorised use of social networking / instant messaging/personal email	X		X		X	X	X	X	X
Unauthorised downloading or uploading of files	X		X		X	X	X	X	X
Allowing others to access school network by sharing username and passwords	X		X		X		X	X	X
Attempting to access or accessing the school network, using another pupil's account	X		X		X	X	X	X	X
Attempting to access or accessing the school network, using the account of a member of staff	X		X		X	X	X	X	X
Corrupting or destroying the data of other users	X		X		X	X	X		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X		X	X		X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X		X			X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X		X			X	X	X	X
Using proxy sites or other means to subvert the school's filtering system	X		X		X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X		X		X	X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X		X	X	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the GDPR.	X		X		X	X	X		X

Trying to access online sites/material that make references to forms of radicalisation	X		X	X	X	X	X	X	

Staff Actions / Sanctions

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

Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X			X
Breaching copyright or licensing regulations		X	X	X	X			X
Continued infringements of the above, following previous warnings or sanctions		X	X	X				X

Recent Guidance

The policy has been reviewed following the latest guidance in KCSIE 2024.

Date on which policy was approved: March 2025
Policy Renew Date: Staff and Governors - February 2025
Policy Review Date: February 2025