e-Safety Policy

2016/2017

The aim of this policy is to ensure appropriate and safe use of the internet and other digital technology devices by all pupils and staff. It details the controls in place to prevent any harmful risks through the provision of a safe learning and teaching environment.

Contents

Scope of the Policy

This policy applies to all members of the multi academy trust community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT 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 cyber-bullying, 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 Policy.

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

Roles and Responsibilities

Board of Directors:

Directors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Directors receiving regular information about e-safety incidents and monitoring reports. A member of the Board has taken on the role of Safeguarding governor which combines e-Safety.

Executive Headteacher, Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the Assistant Headteachers.
- The Executive Headteacher, the Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that staff receive suitable training to enable them to have a full understanding of e-safety procedures so that they can carry out their roles and responsibilities appropriately (see below).
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role.
- The Headteacher provides or coordinates training and advice for staff.

Designated Child Protection Lead will:

- take day to day responsibility for e-safety 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 e-safety incident taking place
- liaises with the Local Authority / relevant body
- liaises with technical support staff
- receives reports of e-safety incidents and records a log of incidents as part of the initial referral system

ICT Technical support:

The ICT technical support team is 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 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
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher.
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Agreement
- they report any suspected misuse or problem to the Headteacher
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- pupils understand and follow the e-safety and acceptable use policies
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Pupils:
- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school.

Parents / Carers:

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

- digital and video images taken at school events
- social media and networking sites and apps (e.g. *WhatsApp*)

e-Safety Education

Education - Pupils

Staff should reinforce e-safety messages across the curriculum. The computing curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of the computing modules.
- Key e-safety messages should be reinforced as part of a planned programme of assembly.
- Pupils should be taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils should be 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
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that 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.

Education - Parents / Carers

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

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

- *School website and school social media platforms*
- *Letters, newsletters*
- *Parents / Carers evenings*
- *Projects and events e.g. Safer Internet Day*

Education & Training – Staff / Volunteers

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

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.

Training - Governors / Directors

Governors / Directors should take part in e-safety training / awareness sessions, whether this is attendance to staff or parent sessions organised by the school.

e-Safety Control Measures

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 school 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 Concero Technology Services 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 year.
- The "master / administrator" passwords for the school ICT system, used by Concero Technology Services must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe)
- Concero Technology Services are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- 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 has provided enhanced / differentiated user-level filtering (senior leaders/staff/pupils).
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual or potential technical incident / security breach to Concero Technology Services.
- 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 process is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) for limited access to school systems.
- The Staff Code of Conduct details the extent of personal use that staff and their family members are allowed on school devices that may be used out of school.
- The acceptable use agreement for staff clarifies the extent to which staff can download executable files and install programmes on school devices.
- School systems will only allow access to removable media that meets certain security criteria. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Communications

When using communication technologies, the multi academy trust 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 through Securus Monitoring Software.
- Users must immediately report, to a senior member of staff, 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 must be professional in tone and content. These communications may only take place through official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may be used at KS1, while pupils at KS2 can be provided with individual school email addresses for educational use.
- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website or social media outlets and only official email addresses should be used to identify members of staff.

Further clarification for staff use of mobile communication technologies is detailed in the Staff Code of Conduct.

Digital Images and Video

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. 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 in 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 pupils in the digital / video images.
- Staff and volunteers permitted 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 unless with prior approval from the Headteacher, as detailed in the Staff Code of Conduct.
- Care should be taken when taking digital video and images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- 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 school social media site, particularly in association with photographs.
- Permission from parents or carers will be obtained before photographs of pupils are published on the school website (School Admission Form)

Data Protection

Schools are recognised as Data Controllers responsible for the management and processing of personal data. This may include information that relates to its pupils, parents and carers, members of staff, and any other individuals who do business with, or come into contact with the school

Personal data is defined as information which relates to a living individual who can be identified from that data or other information held.

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

1. processed fairly and lawfully;
2. obtained only for one or more specified and lawful purpose;
3. adequate, relevant and not excessive;
4. accurate and where necessary, kept up to date;
5. processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. processed in accordance with the rights of data subjects under the Data Protection Act 1998 (DPA);
7. kept secure i.e. protected by an appropriate degree of security;
8. not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data 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" outlined in the DPA
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the DPA.
- 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
- Data Processing Agreements are in place between the Data Controller and third parties who may be contracted to support with the processing of personal data
- 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:

- Keep personal data safe at all times, 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, habitually using *windows key +L* when leaving a school laptop.
- Transfer data using encryption and secure password protected devices
- Immediately report any issue relating to the loss, unauthorised sharing or disclosure of personal data

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

- the device must be encrypted and where appropriate the file should be 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 once it has been transferred or its use is complete

Social Media – Protecting Personal Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies 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 school 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 multi academy trust
- 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 senior staff, marketing, communications and technology manager and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Cyber Bullying

For the purpose of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images online. The school recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.
The school will regularly educate staff, pupils and parents / carers on the importance of staying safe online, as well as being considerate to what they post online. Pupils will be educated about online safety through teaching and learning opportunities as part of a broad and balanced curriculum; this includes covering relevant issues within PSHE lessons as well as sex and relationship education.
The school will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils. There is zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our Behaviour and Discipline Policy. The Headteacher will decide whether it is appropriate to notify the police of the action taken against a pupil.

Reporting Misuse

The multi academy trust clearly defines what is classed as inappropriate behaviour in the Acceptable Use Agreement, and Staff Code of Conduct, ensuring all pupils and staff members are aware of what behaviour is expected of them.

Inappropriate activities are discussed and the reasoning behind prohibiting activities due to e-safety are explained to pupils as part of the curriculum in order to promote responsible internet use.

Misuse by pupils:

- Teachers have the power to discipline pupils who engage in misbehaviour with regards to internet use.
- Any instances of misuse should be immediately reported to a member of staff, who will then report this to a senior leader or the Headteacher.
- Any pupil who does not adhere to the rules outlined in our Acceptable Use Agreement and is found to be wilfully misusing the internet, will have a letter sent to their parents explaining the reason for suspending their internet use.
- Members of staff may decide to issue other forms of disciplinary action to a pupil upon the misuse of the internet. This will be in line with the school Behaviour and Discipline policy and discussed with the Headteacher and will be issued once the pupil is on the school premises.
- Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material, shall be dealt with in accordance with our Child Protection and Safeguarding Policy.

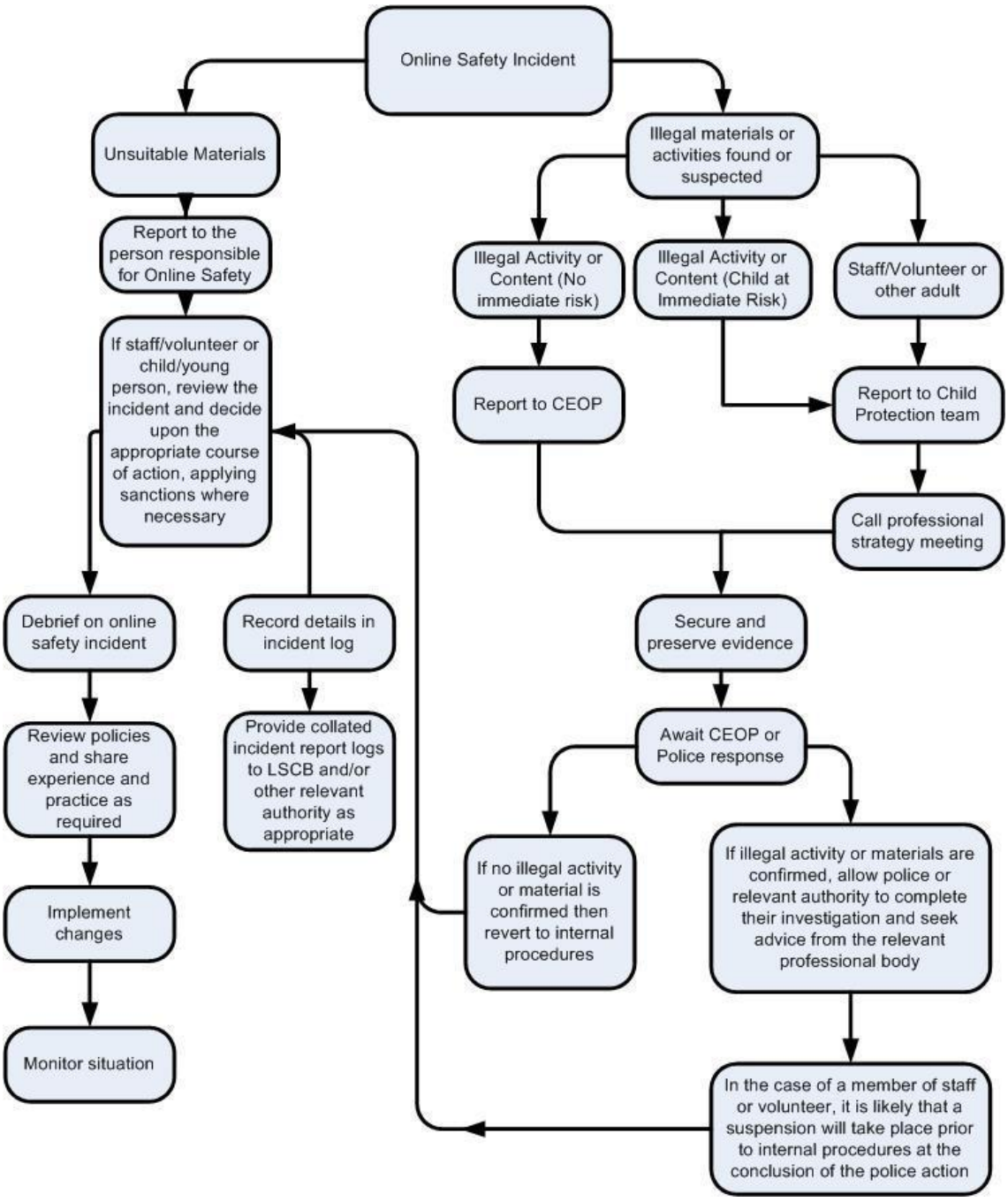
Misuse by staff:

- Any misuse of the internet by a member of staff should be immediately reported to the Headteacher.
- The Headteacher will deal with such incidents in accordance with the conditions of service for staff, and may decide to take disciplinary action against the member of staff.
- The Headteacher will decide whether it is appropriate to notify the police of the action taken against a member of staff.

Use of illegal material:

- In the event that illegal material is found on the school's network, or evidence suggest that illegal material has been accessed, the police will be contacted.
- Incidents will be immediately reported to the Internet Watch Foundation and the police will be contacted if the illegal material is, or is suspected to be, a child sexual abuse image hosted anywhere in the world, a non-photographic child sexual abuse image hosted in the UK, or criminally obscene adult content hosted in the UK.
- If a child protection incident is suspected, the school's child protection procedure will be followed – the DCPL and Headteacher will be informed and the police contacted.

Responding to incidents of misuse - flow chart



Monitoring and Review

This e-safety policy was approved by the Board of Directors	
The implementation of this e-safety policy will be monitored by the:	e-Safety committee of St Martin's multi-academy trust
The Board of Directors will receive reports on the implementation of the e-safety policy, through the usual reporting arrangements, which will include anonymous details of any e-safety incidents	Every 12 months
The e-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Paul Cooper, LADO

The school will monitor the impact of the policy using:

- Monitoring logs of internet activity (including sites visited and any reported incidents) using *Securus monitoring software*
- Internal monitoring data for network activity
- Surveys / questionnaires of pupils, parents / carers and staff