

ST CLEMENT'S C. OF E. ACADEMY

E-SAFETY POLICY

Aims of the Policy

St Clement's Academy embraces the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated communications technologies. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. To that end, St Clement's Academy aims to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

Scope

This policy and related documents apply at all times to fixed and mobile technologies owned and supplied by the Academy and to personal devices owned by adults and young people while on the Academy premises.

Roles and Responsibilities

In this document, the term staff refers to all employees of the Academy, adults that work with the Academy, such as adults in training (students, work experience students), visitors and supply staff, using new technologies on site. The Principal and Governors have ultimate responsibility for establishing safe practice and managing e-Safety issues at our Academy. The role of e-Safety co-ordinator has been allocated to Rob Senior (ICT Co-ordinator) or in his absence the DSL or a member of the Senior Leadership team. They are the central point of contact for all e-Safety issues and will be responsible for day to day management of e-safety in the Academy.

The role of the E-Safety Co-ordinator will include:

- Leading the e-safety committee.
- Taking day to day responsibility for e-safety issues as well as reviewing the Academy e-safety policy.
- Ensuring all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Providing training and advice for staff.
- Liaises with Link to ICT.
- Receiving reports of e-safety incidents and creating a log of incidents to inform future e-safety developments.
- Meeting regularly with the E-Safety Governor.
- Reporting regularly to the SLT.

However, all members of the Academy community have certain core responsibilities within and outside the Academy environment. They should:

- Use technology responsibly.
- Accept responsibility for their use of technology.
- Model best practice when using technology.

- Report any incidents to the e-Safety coordinator and DSL using the Academy procedures.
- Understand that network activity and online communications are monitored, including any personal and private communications made via the Academy network.
- Be aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action.
- Teach internet safety through the Dot Com PHSE programme from Year one to Year six (Pastoral Team).
- Run Internet Safety workshops for parents one a term (Pastoral Team).
- Support the annual E- Safety awareness week (all staff).

Additional roles and responsibilities are discussed in the Becta document - AUP's in context: Establishing safe and responsible behaviours, also available at <http://www.bgfl.org/esafety>. These will be communicated to the relevant groups at appropriate times.

Information System Security

- The security of the Academy's information systems is reviewed regularly.
- Virus protection will be installed and updated regularly.
- The Academy uses broadband with firewall and filters.

Academy Website

- The ICT coordinator and Principal will take overall editorial responsibility for content on the Academy website and ensure it is accurate and appropriate.

Publishing pupils images and work

- Written permission from parents or carers will be obtained at the start of the academic year before photographs of pupils are published on the Academy's website or newsletter. All photographs will be carefully selected.
- Pupil's full names will not be displayed anywhere on the Academy website or in the newsletter alongside photographs.

Social networking and personal publishing

- Social networking sites are blocked on the Academy network.
- Pupils are advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside Academy is inappropriate for primary aged pupils as the popular social networking sites have a minimum age of 13.

Managing Filtering

- The Academy works in partnership with the service provider and BGFL to ensure filtering systems are as effective as possible.
- If staff or pupils discover unsuitable sites, the Academy Forensic software (Policy Central) will automatically capture a screen shot of that site and it will be automatically sent to the Principal where they will determine action required

Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in Academy is allowed.

Evaluating Risks

- The Academy will take all reasonable precautions to ensure that users only access appropriate material. However, due to the world wide scale and linked nature of the Internet, it is not possible to guarantee that unsuitable material will never appear on a Academy iPad or computer. The Academy cannot accept any liability for the material accessed or any consequences of Internet access.
- The e-safety group, with wide representation from Senior Leadership, staff, governors and pupils, will deal with issues relating to e-safety. It will meet regularly to monitor and review e-safety issues and related policies. The e-safety incident log will be reviewed and any actions required in response to this will be discussed and organised.
- The Principal and the ICT coordinator will ensure the E-safety Policy is implemented and compliance with the policy is monitored.

E-Safety Reporting Systems and Sanctions

- Any e-safety issues or complaints must be reported to the e-safety coordinator. These will then be passed on to the Principal.
- Users will have an awareness of how to report issues online, including to CEOP.
- Sanctions are in place for any e-safety abuse or misuse and parents will be informed as relevant.
- Any complaint of a child protection nature must be dealt with in accordance to the Academy's Child Protection and Safeguarding procedures.

Communication of the E-Safety Policy and Raising awareness

- Guidelines for safe Internet use will be discussed with all pupils and displayed in all classrooms.
- Pupil will be informed that Internet use will be monitored about the importance of safe, responsible and confident use of electronic media. Children and staff need to be aware of:
 - The need for caution when putting personal information on the web, including an understanding of what personal information is; address, Academy name, email address, phone number.
 - The need to think carefully before putting any information or pictures online.
 - Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
 - Staff will support the efforts of parents to safeguard the welfare of their children.

Further guidance for staff can be found in the staff handbook.

Cyberbullying

- Cyberbullying (along with all other forms of bullying) of any member of the Academy community will not be tolerated.
- All incidents of cyberbullying reported to the Academy will be recorded.
- All incidents of Cyberbullying will be investigated by the e-safety coordinator and the Principal.
- Pupils, staff and parents/carers are advised to keep a record of the bullying as evidence.
- The Academy will take steps to identify the bully, where possible and appropriate. This may include examining Academy system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the Academy to support the approach to cyberbullying and the Academy's e-Safety ethos.

Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at Academy for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the Academy's anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.

Mobile phones and personal devices

- Mobile phones are not permitted in school for pupils.
- Mobile phones and personal devices must not be used during lessons time or meetings by Academy staff.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the Academy community and any breaches will be dealt with as part of the Academy discipline/behaviour policy.
- Academy staff may confiscate a phone or device if they believe it is being used to contravene the Academy's policy.
- The phone or device might be searched by the Senior Leadership team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
- Electronic devices of all kinds that are brought in to Academy are the responsibility of the user. The Academy accepts no responsibility for the loss, theft or damage of such items. Nor will the Academy accept responsibility for any adverse health effects caused by any such devices either potential or actual.

Pupils Use of Personal Devices

- Pupil's mobile phones will be kept in the Academy office.
- Mobile phones and devices will be released to parents/carers in accordance with the Academy policy.

- If a pupil needs to contact his/her parents/carers during the day they will be allowed to use a Academy phone. Parents cannot contact their child via their mobile phone during the Academy day; they must contact the Academy office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the Academy in a professional capacity.
- Mobile Phones should be switched off or switched to 'silent' mode if they are in classrooms. On no account should a member of staff use the phone for personal use in class.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones, cameras or i-pads to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the Academy policy then disciplinary action may be taken.

How will the policy be shared with pupils?

- All users will be informed that network and Internet use will be monitored.
- An e–Safety training programme will be established across the Academy to raise the awareness and importance of safe and responsible internet use amongst pupils.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- An e–Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe Academy and home use.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Particular attention to e-Safety education will be given where pupils are considered to be vulnerable.

How will the policy be discussed with staff?

- The e–Safety Policy will be formally provided to and discussed with all members of staff.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.

- Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- The Academy will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
- All members of staff will be made aware that their online conduct out of Academy could have an impact on their role and reputation within Academy. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

How will parents' support be enlisted?

- Parents' attention will be drawn to the Academy e-Safety Policy in newsletters, the Academy prospectus and on the Academy website.
- A partnership approach to e-Safety at home and at Academy with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e-Safety at other attended events e.g. parent evenings and sports days.
- Information and guidance for parents on e-Safety will be made available to parents in a variety of formats.
- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations listed in the "e-Safety Contacts and References section" such as CEOP (Child Exploitation and Online Protection Centre): www.ceop

How will the Academy respond to any incidents of concern?

- All members of the Academy community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The e-Safety Coordinator will record all reported incidents and actions taken in the Academy e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The DSL will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The Academy will manage e-Safety incidents in accordance with the Academy discipline/ behaviour policy where appropriate.
- The Academy will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the Academy will debrief, identify lessons learnt and implement any changes required. Where there is cause for concern or fear that illegal activity has taken place or is taking place then the Academy will contact the Children's Safeguard Team or e-Safety officer and escalate the concern to the Police.
- If the Academy is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Safeguarding Board or the Academy Sponsor.

How will e–Safety complaints be handled

- Complaints about Internet misuse will be dealt with under the Academy’s complaints procedure.
- Any complaint about staff misuse will be referred to the Principal.
- All e–Safety complaints and incidents will be recorded by the Academy, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the Academy to resolve issues.
- All members of the Academy community will need to be aware of the importance of confidentiality and the need to follow the official Academy procedures for reporting concerns.
- Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children’s Safeguard Team to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the Academy’s disciplinary, behaviour and child protection procedures.
- All members of the Academy community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the Academy community.

e–Safety Contacts and References

www.ceop.gov.uk The Child Exploitation and Online Protection Centre (CEOP) -brings together law enforcement officers, specialists from children’s charities and industry to tackle online child sexual abuse. CEOP provides a dedicated 24 hour online facility for reporting instances of online child sexual abuse.

www.thinkuknow.co.uk this is a website for young people full of information about staying safe online. It includes areas with practical guidance for parents and carers, and for teachers and trainers.

www.childnet-int.org Childnet International is an organisation which works with partners around the world to try to ensure that children and young people are protected from the dangers of the Internet.

<http://www.education.gov.uk/ukccis/about> The UK Council for Child Internet Safety (UKCCIS) - this site includes information about the Byron Reviews “Safer Children in a Digital World”

www.virtualglobaltaskforce.com The Virtual Global Taskforce is an international alliance of law enforcement agencies working together to make the Internet a safer place.

www.education.gov.uk/Academys/pupilsupport/behaviour/bullying This site includes advice for Academys on preventing and responding to bullying.

www.iwf.org.uk The Internet Watch Foundation is an organisation which works with the Police and Internet Service Providers to trace those responsible for putting harmful or illegal material on the web.

www.stopitnow.org.uk

www.lscbbirmingham.org.uk Birmingham children's safeguarding board.

Access and review of policy

St Clement's Academy's e-safety Policy is accessible to all staff and the Academy community via the Academy's website. A hard copy is provided in each classroom file. Further hard copies can be obtained through the Academy reception.

The board of governors will review this policy every two years or sooner should guidance change.

Revised: June 2015

Approved: September 2015

Review Date: June 2017



ST. CLEMENT'S
C.OF E. ACADEMY