The Southwater Infant Academy

Online Safety Policy

Author: Christie Cavallo

Date Revised: June 2021

Review Date: June 2022

At The Southwater Infant Academy we will continuously strive to ensure that everyone is treated with respect and dignity. Each person will be given fair and equal opportunities to develop their full potential regardless of their gender, transgender, ethnicity, culture and religious background, sexuality, disability, or special educational needs and ability. The academy will actively promote equality and foster positive attitudes and commitment to an education for equality.

Writing and reviewing the Online Safety policy

The Online Safety Policy is part of the Academy Development Plan and relates to other policies including those for Computing, Communications, Social Media, Behaviour, Data Protection and Safeguarding.

The academy will identify a member of staff who has an overview of Online Safety, this would usually be a member of the Senior Leadership Team (SLT).

Our Online Safety Policy has been written by the academy, building on best practice and government guidance. It has been agreed by senior management and approved by the Board of Trustees.

Responsibilities

Trustees

The Board of Trustees are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. A member of the Trustee Board has taken on the role of **Online Safety Trustee.** The current Online Safety Trustee is Jay Shekleton.

The Senior Leadership Team:

- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments
- provides advice for staff and others and organises training as needed
- liaises with external agencies, particularly in respect of child protection issues arising from online safety work

The Online Safety Co-ordinator:

- takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the academy Online Safety policies / documents
- keeps up-to date with developments in relation to Online Safety and disseminates these widely
- helps ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- helps provide training and advice for staff and others
- liaises with teaching and other staff in developing and evaluating Online Safety educational programmes
- liaises with the Local Authority / other relevant bodies
- liaises with Schools ICT technical staff.
- ensures the academy is complying with GDPR regulations in liaison with the DPO

Technical Staff are responsible for ensuring:

- that the academy's technical infrastructure is secure and is not open to misuse or malicious attack, including regular updating of virus protection
- that the filtering system is applied effectively and consistently
- that user names/ access to academy systems are updated e.g. when informed that a member of staff leaves
- that checks are carried out as required on staff laptops
- 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 technical systems and processes comply with GDPR regulations.

Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of Online Safety matters and of the current Online Safety policy and practices
- they read, understand and sign annually the Staff Acceptable Use Agreement (Appendix One)
- they report any suspected misuse or problem to the Headteacher/ Online Safety Coordinator
- all digital communications with students / pupils / parents / carers are on a professional level and only carried out using official academy systems
- Online Safety issues are embedded in all aspects of the curriculum and other activities
- personal data is handled securely (see e-mail and Data Protection sections below)
- pupils understand and follow the Online Safety and acceptable use policies
- pupils have an understanding of digital literacy and copyright issues appropriate to their age.
- policies and procedures relating to GDPR regulations are read, understood and adhered to.

Teaching and Learning

Why Internet and digital communications are important

The Internet is an essential element in 21st century life for education, business and social interaction. The academy has a duty to provide students with quality Internet access as part of their learning experience.

Internet use is a part of the curriculum and a necessary tool for staff and pupils.

Internet use enhances learning

Pupils are required to return a signed copy of the Pupil Acceptable User Agreement (Appendix Two) every year, which must be countersigned by their parent or carer (in the case of Foundation Stage, parental signature only required).

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation, using a 'child-friendly' search engine.

A planned Online Safety curriculum is provided as part of Computing / PHSE / other lessons and is regularly revisited using a variety of approaches appropriate to the age and maturity of the children.

Pupils are helped to understand the need for the Pupil Acceptable Use Policy and encouraged to adopt safe and responsible use both within and outside academy.

Pupils will be taught how to evaluate Internet content/ Digital Literacy
The academy will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
Pupils are taught to question information before accepting it as true.
Pupils are encouraged to tell a member of staff immediately if they find any material that makes them feel uncomfortable.

Educating parents and other carers
Many parents and carers may have only a limited understanding of Online Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line 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 academy will therefore seek to provide information and awareness to parents and carers through:
Curriculum activities, letters, newsletters, academy web site, parent forums, reference to other relevant web sites / publications

Education and training for staff
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. This will include training for GDPR.
All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the academy 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 (eg from 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 staff meetings / INSET days at least annually.
The Online Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.
All staff will sign our Acceptable Use Agreement on appointment and this will be included in induction packs for volunteers and students.

Trustees education and training
Trustees should take part in Online Safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in technology / Online Safety / health and safety / safeguarding.
This may be offered in a number of ways e.g.: Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation / participation in academy training / information sessions for staff or parents.
Trustee monitoring visits will take place during the year and be reported to the Board of Trustees.

Managing Internet Access

Information system security

Academy ICT systems security will be reviewed regularly.
Virus protection will be updated regularly.
Recommended security strategies will be followed if appropriate.

E-mail

Staff and pupils may only use approved e-mail accounts on the academy system.
Pupils must have adult supervision if using email. Pupils must immediately tell a teacher if they receive offensive or bullying email or any communication which makes them feel uncomfortable. They should not respond to such emails. Staff are not permitted to use academy email addresses for personal business. All email should be kept professional. Staff are reminded that academy data, including emails, is open to Subject Access Requests under the Freedom of Information Act.
Staff must immediately tell the Head teacher if they receive offensive or bullying email or any communication which makes them feel uncomfortable. They should not respond to such emails.
E-mail sent to an external organisation should be professional in tone and content, in the same way as a letter written on academy headed paper. The forwarding of chain letters is not permitted.

Published content and the academy web site

The contact details on the Web site should be the academy address, e-mail and telephone number. Staff or pupils' personal information will not be published.
The Senior Leadership Team will take overall editorial responsibility and ensure that content is accurate and appropriate.
All parents are required to give consent for images of their children to be used online. Any photo titles or captions will not include children's surnames. The option to opt out will be clear and simple for parents at any time.
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 academy events for their own personal use (as such use is not covered by the GDPR). To respect everyone's privacy and in some cases for child 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 academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on academy equipment, the personal equipment of staff should not be used for such purposes. GDPR regulations should be followed at all times regarding the taking, use and storage or images.
Care should be taken when taking digital / video images that pupils are appropriately dressed.

Social networking and personal publishing/Cyber-bullying
Staff, volunteers and students follow the guidelines in the Social Media Policy. All staff are expected to have read this policy and to abide by the guidance. Failure to abide by the guidance could result in disciplinary action.
The academy will block/filter access to social networking sites, except in special circumstances for essential staff access when promoting the academy. Pupils will be 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.
Any incidents of cyber-bullying will be reported directly to the Designated Safeguarding Lead. Any outside agencies such as police will then be notified, child protection procedures will be followed. Any pupil found to be involved with any misuse of the internet at academy or home (including cyberbullying) will have their access to the internet taken away and this will be reviewed regularly. All incidents will be logged and regularly monitored, parents will also be informed.
Other members of the academy community affected by cyberbullying should also be supported by the academy.

Managing filtering
The academy filtering system is provided by Schools ICT.
The academy will work with the Schools ICT support technicians to ensure systems to protect pupils are reviewed and improved.
If staff or pupils discover an unsuitable site, it must be reported to the Computing Subject Leader and Online Safety Co-ordinator.
The Computing Subject Leader/ Online Safety Co-ordinator will ensure that regular checks are made so that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies
Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in academy is allowed. Staff mobile phones are not to be used in the classroom during contact time. Staff cameras and other mobile devices are not to be used during contact time except in an emergency during a trip in order to contact academy. Staff are permitted to take their own mobiles with them on trips in case of personal emergency but they are not to be used routinely.
Parent helpers and others (e.g. students and volunteer)s will be reminded about academy policy on phones and cameras when on trips.

Data Protection
Personal data will be recorded, processed, transferred and made available according to the GDPR. 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.
- Pass any Individual Rights requests to the Headteacher or Deputy Headteacher immediately.

When personal data is stored on any portable computer system:

- The data must be encrypted and / or password protected
- The device must be password protected.

Use of academy ICT equipment away from academy premises
The provisions of this policy apply equally to all academy ICT equipment when used away from academy premises.

Assessing risks
Access to the internet will be by adult demonstration with directly supervised access to specific online resources. The academy will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on an academy computer. Neither the academy nor Schools ICT can accept liability for the material accessed, or any consequences of Internet access.
The academy will audit ICT provision to establish if the Online Safety policy is adequate and that its implementation is effective.

Complaints
Responsibility for handling incidents of internet misuse will be taken by the Headteacher.
Any complaint about staff misuse of digital technology must be referred to the Head teacher.
Complaints of a child protection nature must be dealt with in accordance with academy safeguarding procedures.
Pupils and parents will be informed of the complaints procedure.
There may be occasions when discussions will be held with the police support services to establish procedures for handling potentially illegal issues.
Where possible the academy will liaise with local organisations to establish a common approach to Online Safety.

Communicating the Online Safety Policy
Introducing the Online Safety policy to pupils
Online Safety rules will be posted in all classrooms and discussed with the pupils at the start of each year. Pupils will be informed that network and Internet use will be monitored.

Staff and the Online Safety policy
All staff will be given the Academy Online Safety Policy and Social Media Policy and their importance explained. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.

If a colleague at the academy believes they will have any difficulty complying with any of the requirements in this policy for whatever reason (for example, where they are related to a pupil), they should discuss the matter with the Headteacher/ the academy designated safeguarding teacher/officer. Failure to do so will be regarded as a serious matter.

Parental support
Parents' attention will be drawn to the Academy Online Safety Policy in newsletters and on the academy web site. Parents will be asked to read through the relevant Pupil Acceptable User Agreement with their child and co-sign it on an annual basis.

Appendix 1

Staff (and Volunteer) Acceptable Use Policy Agreement

Academy Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.
- Data Protection requirements under the GDPR are met.

The academy will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the academy will monitor my use of the academy digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, Sharepoint etc.) out of the academy, and to the transfer of personal data (digital or paper based) out of the academy.

- I understand that the academy digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the academy.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may be able to obtain it.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person.

I will be professional in my communications and actions when using academy ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission and always ensure I follow GDPR when doing so.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the academy's policy on the use of digital / video images and with GDPR. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the academy website) it will not be possible to identify by name, or other personal information, those who are featured, and this will only be done are consent has been freely given by the parent / carer.
- I will only use social networking sites in the academy in accordance with the academy's policies.
- I will only communicate with pupils and parents / carers using official academy systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The academy and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the academy:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in the academy, I will follow the rules set out in this agreement, in the same way as if I was using academy equipment. I will also follow any additional rules set by the academy about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the academy ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure that my data is regularly backed up, where this is possible, to a secure space such as OneDrive.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in academy policies.
- I will not disable or cause any damage to academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others as outlined in the academy Data Protection Policy and in compliance with GDPR. Where digital personal data is transferred outside the secure local network, it must be encrypted and /or password protected. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access will be kept private and confidential, except when it is deemed necessary that I am required by law or by academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will immediately report any data breaches, or near misses, to the Headteacher or Deputy Headteacher as soon as I am aware of them.

When using the internet in my professional capacity or for academy sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the academy:

- I understand that this Acceptable Use Policy applies, not only to my work and use of academy digital technology equipment in the academy, but also applies to my use of academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the academy.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to the Board of Trustees and / or the Local Authority and in the event of illegal activities the involvement of the police.

Acceptable Use Policy Agreement

I have read and understood the Online Safety Policy, Social Media Policy and Data Protection Policy. I agree to follow the guidance within these policies, and will use the academy digital technology systems (both in and out of the academy) and my own devices (in the academy and when carrying out communications related to the academy) within these guidelines.

Staff / Volunteer Name: .....

Signed: .....

Date: .....

Appendix 2

Staying Safe Online

This is how we stay safe when we use computers:

- I will ask a teacher or adult if I want to use the computers / tablets.
- I will only use activities that a teacher or adult has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from a teacher or adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer / tablet.

Signed (child): .....

Signed (parent): .....