

**STALHAM ACADEMY**

**E-SAFETY POLICY**

**JUNE 2015**

**Relates to N.M.S.: Standard 11 Child Protection**

The elements of this policy enable the Academy to demonstrate that its e-Safety

Policy is compliant with the Norfolk E-Safety Group approved policy. Naturally policy must be translated into practice to protect pupils and educate them in responsible ICT use.

**Who writes and reviews this policy?**

The e-Safety Policy relates to other policies including ICT Acceptable Use, and Behaviour.

The Academy has appointed an e-Safety Coordinator. Our E-Safety Policy has been written by the Academy in conjunction with the Trust, building on the NCC e-Safety Policy and government guidance. It has been agreed by the senior management and approved by the governors.

The e-Safety Policy and its implementation will be reviewed annually, to include changes in the use of technology, its benefits and risks.

**How can we safely use the Internet to enhance learning?**

Staff can help pupils to learn how to distil the meaning from the mass of information provided by the Internet. Often the quantity of information is overwhelming and staff may guide pupils to appropriate websites, or teach search skills. Offering younger pupils a few good sites is often more effective than an Internet search. Above all pupils need to learn to evaluate everything they read and to refine their own publishing and communications with others via the Internet.

* The Academy Internet access will be designed expressly for pupil use and will include very strict filtering appropriate to the needs of the curriculum.
* Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
* Internet access will be planned to enrich and extend learning activities.
* Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
* Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils’ age and maturity.
* Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

**How will pupils learn how to evaluate Internet content?**

As part of the Computing Curriculum pupils should be taught research techniques and be encouraged to question the validity, currency and origins of information. Pupils should compare web material with other sources. Effective guided use will also reduce the opportunity pupils have for exploring unsavoury areas.

In a perfect world, inappropriate material would not be visible to pupils using the Internet, but this is not easy to achieve and cannot be guaranteed, even with filtering. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example: to close the page and report the incident immediately to the teacher.

Respect for copyright and intellectual property rights, and the correct use of published material should be taught.

The Academy endeavours to ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

* Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
* Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
* The evaluation of on-line materials is a part of every subject.

**Managing Information Systems**

**How will information systems security be maintained?**

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services, but also the personal safety of staff and pupils.

ICT security is a complex matter and cannot be dealt with adequately in this document. A number of agencies can advise on security including Becta and the Trust’s IT Department.

Local Area Network security issues include:

* Users must act reasonably – e.g. the downloading of large files during the working day will affect the service that others receive.
* Users must take responsibility for their network use. Breaching the Staff Acceptable Use ICT policy (AUP) may result in disciplinary action.
* Workstations should be secured against user mistakes and deliberate actions.
* Servers must be located securely and physical access restricted where possible.
* The server operating system must be secured and kept up to date.
* Virus and Spyware protection will be installed and updated regularly.
* The Academy’s domain uses 256bit SSL encryption and SSL interception is active on our safeguarding filters.

Access by wireless devices must be pro-actively managed. Wide Area Network (WAN) security issues include: All Internet connections must be arranged via the Network Manager to ensure compliance with the security policy. The Academy’s firewalls, routers and switches are configured to prevent unauthorised access between Academy’s network and the wider internet.

The following precautions will be reviewed annually;

* The security of the Academy Information Systems will be reviewed regularly by the Head of School and Network Manager.
* Virus, Malware and Spyware protection will be installed and updated regularly by the ICT technician.
* Login details must not be shared
* Personal data sent over the Internet will be encrypted or otherwise secured by individual logins and passwords.
* Unapproved system utilities and executable files will not be allowed in pupils’ work areas or attached to e-mail.
* The Network Manager will review system capacity regularly.

**How will e-mail be managed?**

E-mail is an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects between Schools/Academies locally, nationally and internationally.

The implications of e-mail use for the Academy and pupils need to be thought through and appropriate safety measures are put in place by the Academy such as;

* Individual email accounts supplied for pupil
* AUP for students
* Monitoring of email system via access to the VLE
* Ability to lock down and monitor email accounts from a central location

Un-regulated e-mail can provide routes to pupils that bypass the traditional Academy boundaries/filters and no information audit trail therefore pupils and staff are not permitted to use private email addresses for Academy purposes.

In the Academy context, e-mail should not be considered private and the Trust reserve the right to monitor e-mail. There is a balance to be achieved between necessary monitoring to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

E-mail accounts are constructed for pupils as zzblue@stalhamacademy.co.uk as it is safer for children, to disguise identities. Pupil accounts are restricted to receiving and sending emails to @stalhamacademy.co.uk addresses only. Incoming/Outgoing email from outside the Academy to/from a pupil account will be rejected.

All inbound and outbound emails (including attachments) are filtered for objectionable content and are blocked should this be found; one example of this would be profanity, but this also reduces access to cyberbullying whilst at school.

The Academy’s Broadband Network and services provided on this network have security in place to reduce the impact of SPAM, phishing, viruses and other malware.

Users may only use approved e-mail accounts.

Users must immediately tell a teacher if they receive offensive e-mail.

Users must not send jokes or other materials that the receiver may find offensive

Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

Access in the Academy to external personal e-mail accounts should be blocked.

Excessive social e-mail use can interfere with learning and may be restricted.

E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on Academy headed paper.

The forwarding of chain letters is not permitted.

**How will published content be managed?**

Stalham Academy has created a website and classrooms that inspire pupils to publish work of a high standard. Editorial guidance will help reflect the Academy’s requirements for accuracy and good presentation.

Publication of sensitive information should be considered from a personal and Academy security viewpoint before being published on the Academy website and guidance should be sought from the Network Manager or Head of School.

The contact details on the website should be the Academy address, e-mail and telephone number. Staff or pupils’ personal information must not be published.

E-mail addresses should be published carefully, to avoid spam harvesting by web crawlers.

The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

The website should comply with the statutory policies for academies as identified by the DFE.

**Can pupil’s images or work be published?**

The publishing of pupils’ names with their images is not acceptable. Strategies include using relatively small images of groups of pupils and possibly even using images that do not show faces at all. Personal photographs can be replaced with self-portraits or images of pupils’ work or of a team activity. Pupils in photographs should, of course, be appropriately clothed.

Images of a pupil should not be published without the parent’s or carer’s written permission. Stalham Academy asks permission to publish images of work or appropriate personal photographs at the time of admission to the Academy. Further clarification for publicly displayed work is sometimes individually sought.

Pupils are taught the reasons for caution in publishing personal information and images in social publishing sites. Pupils’ full names will not be used anywhere on the website or blog, particularly in association with photographs.

**How will social networking and personal publishing be managed?**

In order to promote safety, the Academy will block/filter access to social networking sites and monitor use of ICT in the classroom. No pupil should be allowed access to a computer by themselves whilst within Academy. Pupils who contravene the AUP will be subject to an ICT ban for a set period of time.

As part of eSafety lessons pupils should be encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo or address once published on gaming and social networking platforms. Pupils and staff are advised never to give out personal details of any kind which may identify themselves or others and / or their location (Please see AUP for staff and pupils). Examples would include real name, address, mobile or landline phone numbers, Academy attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc. Pupils should be advised to use avatars and nicknames to reduce dangers.

Teachers’ official blogs or wikis should be password protected and run from the Academy classroom or website. Any interaction, involving the school, between pupils, parents and staff should be through the Academy email, classrooms or school phones.

All users are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Users should be encouraged to invite known friends only and deny access to others.

Users are advised not to publish specific and detailed private thoughts.

All staff and pupils should be aware of and deal with bullying that can take place through social networking. The inclusion of within text messages is difficult for staff to detect. Pupils may need reminding that inappropriate language or images is both inappropriate and conflicts with Academy policy. Abusive messages may be dealt with under the Academy Anti-bullying policy.

Parents are only given permission to photograph their own children. They are not to:

* post photos, videos or comments that include other children at the school
* use social media on their own devices while on school premises
* access social media while helping at school or on school visits
* post anything malicious about the school or any member of the school community

Any queries, concerns and complaints should be voiced directly with the school rather than posting them on social media – whether on parents’ own pages or in closed groups.

If the school is made aware of such happenings, the parents will be contacted by the academy and asked to remove the content. If parents continue to break the rules, the academy will ultimately ban photos and videos from school events.

If a parent is accused of making malicious comments about the school or a teacher on social media, in accordance with government advice, the parent will be invited to a meeting with the school. This will be addressed through the usual complaints procedure – but the school can request that the offensive comments are removed. If the parent refuses, the school can escalate the matter by reporting it to the social networking site or the local authority, or can seek legal advice. Comments that are threatening, abusive, racist, sexist or that could be seen as a hate crime can be reported to the police as online harassment.

**How will filtering be managed?**

Internet access must be appropriate for all members of the Academy community.

To restrict access to inappropriate material there are multiple blocking strategies. This is via Safetynet Plus for active internet content filtering, backed up by Securus for local content (documents etc). Maintenance of the filtering is overseen by the Network Manager.

Attempted access to a site forbidden by the policy or use of inappropriate language/images in a document will result in a report, parents being contacted and an ICT ban for a specified period of time.

The Head of School will be made aware of filtering profile changes by the Network Manager

If staff or pupils discover unsuitable sites, the URL must be reported to the Network Manager or Head of School.

The Network Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable and report back to the Head of School.

Any material that the Academy believes is illegal must be reported to appropriate agencies such as IWF or CEOP, the Network Manager and Head of School.

**How will videoconferencing be managed?**

Videoconferencing is not used in the Academy at the present. If this activity was to be useful to the learning, then the risks will be considered and become part of this policy.

**How should personal data be protected?**

The Data Protection Act 1998 gives individuals the right to know what information is held about them and it provides a framework to ensure that personal information is handled properly.

Data Protection information may be seen at:

Commissioner’s Office: http://www.ico.gov.uk/

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

**How will Internet access be authorised?**

The Academy allocates Internet access on the basis of educational need. Most pupils will be granted Internet access, however at times pupils will be denied access following an ICT ban. (Appendix; AUP policy for Staff and Pupils) Parents/carers will be informed in all cases.

The Academy will maintain a current record of all staff and pupils who are granted access to the Academy’s electronic communications.

All staff must read and sign the ‘Staff Acceptable Use Policy for ICT’ (AUP) and read the guidance before using any Academy ICT resource.

On using the school technology, pupils will agree to the Acceptable Use Policy for ICT (AUP).

**How will e-safety complaints be handled?**

Where necessary the complaints policy and disciplinary procedures will be followed in accordance with the Academies complaints procedure.

**How the internet is used by the Academy in the community**

The Academy will liaise with other trust schools to establish a common approach to e-safety.

The Academy will be sensitive to Internet related issues experienced by pupils out of Academy, e.g. social networking sites, and offer appropriate advice.

Community users coming into Academies must adhere to the Academy’s E-safety policy.

**How will the policy be discussed with staff?**

Staff must sign the AUP (Acceptable Use Policy) in relation to this policy. It is important that all staff feel confident to use new technologies in teaching. The Academy e-Safety Policy will only be effective if all staff subscribe to its values and methods therefore staff are expected to raise any queries relating to this policy with the Network Manager/Head of School. If a member of staff is concerned about any aspect of their ICT use in the Academy, they should discuss this with the Head of School to avoid any possible misunderstanding.

ICT use is widespread and all staff including administration, caretaker, governors and helpers should be included in appropriate awareness raising and training. Induction of new staff and regular supply must include a briefing of the Academy’s E-Safety/Acceptable Use Policy.

All staff will be given the Academy e-Safety Policy and its application and importance explained.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Staff training in safe and responsible Internet use and on the Academy e-Safety Policy will be provided as required.

**How will parents’ support be enlisted?**

Parents’ attention will be drawn to the Academy’s e-Safety Policy in newsletters, the Academy brochure and in the initial admissions papers.

Internet issues will be handled sensitively, and parents will be advised accordingly.

Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

**Mobile Technology Guidance**

Pupils’ use of personal devices

* Pupils are not permitted to use personal devices during the school day or on school property.
* All mobile phones and personally-owned devices should be handed in to reception or locked away in secure storage if they are brought into school.
* If permission is granted at any time eg. During a residential, parents will sign a bespoke agreement form.
* If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone.
* Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school 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 and encouraged to use PIN’s and other security as necessary.

Staff use of personal devices

* Staff are not permitted to use their own mobile phones or devices for contacting pupils, young people or those connected with the family of the student.
* Staff will be issued with a school phone where contact with pupils, parents or carers is required, for example a mobile on school trips or staff based landline in departments or school offices. Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then a school mobile phone will be provided and used. In an emergency where the staff member doesn’t have access to a school owned device, they should use their own devices and hide (by inputting 141) their own mobile numbers for confidentiality purposes.
* Mobile phones and personally-owned devices will be switched off or switched to ‘silent’ mode, Bluetooth communication should be ‘hidden’ or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
* Approval by a member of the senior leadership team must be explicitly given before children may use mobile phones or a personal device as part of an educational activity. Generally there will be a good educational reason for the activity to take place.
* Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use school provided equipment for this purpose. If for any reason it has been necessary to use a personal device to take an image of a child, this will be downloaded onto the school network and deleted from the personal device in the presence of the DSL by the end of the school day.
* If a member of staff breaches the school policy then disciplinary action may be taken as appropriate.
* Staff use of mobile phones during the school day will be limited to the lunch break and after school.
* Mobile phones should be switched off and left in a safe place during lesson times. Staff should use mobile phones in designated areas. The designated areas are the staff room and the school office. If a private call needs to be made then a request for a room can be made to the Senior Leadership Team or the school office.
* Staff should ensure that their phones are protected with PIN/access codes in case of loss or theft.
* Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
* Staff should not send and receive texts in classrooms or use camera phones at any time.
* Staff should never contact students from their personal mobile phone, or give their mobile phone number to students. If a member of staff needs to make telephone contact with a parent, a school telephone should be used.
* Staff should never store parents’ or pupils’ telephone or contact details on their mobile phone, as this allows the possibility of inappropriate contact.
* Staff should never send, or accept from anyone, texts or images that could be viewed as inappropriate.
* If a member of staff suspects a message, text or similar may contain inappropriate content it should not be opened but a senior member of staff, preferably the e-safety coordinator or DSL should be contacted.