E-Safety

Long Stratton High School

Policy Consultation & Review

The E-Safety Policy is part of the School's priority to keep children safe. It forms part of the school's safeguarding procedures and relates to other policies including those for bullying, communication, mobile phone usage and safeguarding.

The E-Safety policy was created in consultation with key staff and students.

This policy will be reviewed in full by the Governing Body on an annual basis. This policy was last reviewed and agreed by the Governing Body in January 2019. It is due for review in January 2020.

Signature Headteacher Date:

Signature Chair of Governors Date:

Contents

Related policies/documents

- Legal Framework
- ICT Acceptable Use Policy (Students) (AUP)
- ICT Acceptable Use Policy (Staff, Visitors, Governors) (AUP)
- Photograph, Internet and Video Parent Consent Form.
- Example Parent/Carer ICT Code of Conduct agreement form (Feb 2016)
- Guidance on the use of CCTV in schools including the Use of Fixed Video Cameras in the Classroom (Colin Burton)
- Mobile Telephone Agreement for pupils.

1. Introduction and Overview
Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Long Stratton High School with respect to the use of technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of technologies for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying and ensure that these structures run in conjunction with procedures in other relevant school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms

The online safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy).

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the Senior Leadership Team (SLT) and approved by Governors. All amendments

to the school online safety policy will be disseminated to all members of staff and pupils.

2. Education and Curriculum
Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the ICT curriculum. This covers a range of skills and behaviours appropriate to their age and experience.
- will remind students about their responsibilities through the pupil ICT Code of Conduct/ Acceptable Use Agreement(s)
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights

Staff and governor training

This school:

- makes up to date training available to staff on online safety issues and the school's online safety education program
- provides, as part of the induction process, all staff (including those on university/college placement and work experience) with information and guidance on the Online Safety Policy and the school's ICT Code of Conduct/ Acceptable Use Agreements

Parent/Carer awareness and training

This school:

- provides information for parents/carers for online safety on the school website

3. Incident management
In this school:

- There is strict monitoring and application of the online safety policy, including the ICT Code of Conduct and a differentiated and appropriate range of sanctions support is actively sought from other agencies as needed (i.e. the local authority, UK Safer Internet Centre Helpline, CEOP, Police, Child Net) in dealing with online safety issues

- Monitoring and reporting of online safety incidents takes place and contributes to developments in policy and practice in online safety within the school
- Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law
- we will immediately refer any suspected illegal material to the appropriate authorities – i.e. Police, CEOPs.

4. Managing IT and Communication System
Internet access, security and filtering

In this school:

- We follow guidelines issued by the Department for Education to ensure that we comply with minimum requirements for filtered broadband provision. By following the Education Network (NEN) school e-security checklist, we will ensure that the school networks are kept secure and protected from internal and external threats.

E-mail
This school:

- We provide staff with an email account for their professional use, e.g. lshs.org.uk and make clear personal email should be through a separate account
- We use anonymous e-mail addresses, for example head@, office@
- We will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date

Pupils' email:

- We use school provisioned pupil email accounts that can be audited
- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff email:

- Staff will use LA or school provisioned e-mail systems for professional purposes
- Access in school to external personal email accounts may be blocked

- Never use email to transfer staff or pupil personal data outside of the school unless it is protected with secure encryption. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

School website

- The school web site complies with statutory DfE requirements
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs of pupils published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- The use of any school approved social networking will adhere to ICT Code of Conduct/Acceptable Use Policy

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to sign and follow our pupil ICT Code of Conduct/AUP

.

Parents/Carers:

- Parents/carers are reminded about social networking risks and protocols through our parental ICT Code of Conduct/AUP and additional communications materials when required.

5. Data Security

Management Information System access and data transfer

- We follow the guidance from the Information Commissioner's Office to ensure that we comply with our responsibilities to information rights in school. We will ensure that we regularly check that we are compliant.

6. Equipment and Digital Content
Digital images and video

In this school:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs
- Staff sign the school's ICT Code of Conduct/Acceptable Use Policy and this includes a clause on the use of personal mobile phones/personal equipment
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term, high profile use.