E-Safety Policy (Trust including EYFS)

Related Policies

- E-Safety Pupil Acceptable Use Policy and Guidelines
- E-Safety Staff Acceptable Use Policy and Guidelines
- Keeping Children Safe in Education (2018)
- Taking, Storing and Using Images of Children Policy
- Staff Code of Conduct

1. Introduction

I. The internet and other digital technologies are powerful tools which open up new opportunities for everyone. These technologies promote the requirement to ensure that pupils are able to use the internet and related communication technologies appropriately and safely. This needs to be addressed as part of the wider duty of care, to which all who work in schools are bound.

II. This policy applies to all members of the school community (including staff, pupils and volunteers) who have access to and are users of school ICT systems, both in and out of school.

III. 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.

IV. This is pertinent to incidents of cyber-bullying, or other e-safety incidents which may take place out of school, but are linked to membership of the school.

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

2. Responsibilities:

a) Governors:

An e-Safety specific Governor will be appointed and shall undertake to:

a) Meet with the E-Safety Co-ordinator at pre-arranged times
b) Monitor the e-Safety incident logs at regular intervals
c) Report to relevant governor's meetings

b) Headmasters and SMT:

I. The Headmasters of both schools are responsible for ensuring the safety of members of the school community. Though the day to day responsibility for e-Safety will be delegated to the Principal Deputy Head (Senior), Deputy Head (Prep) and the e-Safety Co-ordinators.

II. The Headmasters in conjunction with the Deputy Head (Senior) and Deputy Head (Prep) are responsible for ensuring that relevant key staff are suitably trained through CPD events.

III. The Headmasters and respective SMT's will receive regular monitoring reports from the E-Safety Co-ordinator.

IV. The Headmasters and SMT's should be aware of the procedures to be followed (as laid out in the Trust Incident Flow Chart, see Appendix 1) in response to a serious e-safety allegation being made against a member of staff

c) E-Safety Co-ordinators

I. The Trust shall have appointed E-Safety Co-ordinators who report directly to the Principal Deputy Head (Senior) and Deputy Head (Prep) with regards to e-Safety incidents and any child protection concerns in their respective settings.

Senior:

a) Assists under guidance from the Headmaster and Principal Deputy Headmaster with regulatory inspections
b) With the Senior Management Team establishes and supports incident management processes
c) Takes day- to- day responsibility for e-safety issues
d) Maintains incident logs of reported e-safety incidents
e) Maintains a Social Media Register and monitors the use of Social Media, reporting any incidents
f) Ensures that all staff, academic and non – academic, are briefed on e-Safety responsibilities and procedures
g) Provides training and support for staff, governors, parents and pupils raising awareness of e-Safety
h) Meets once a term with the e-Safety Governor, Principal Deputy Head and Head of IT Services to discuss current status and to review incident logs

Prep:

a) Leads and co-ordinates the e-Safety committee
b) Assists under guidance from the Headmaster and Principal Deputy Headmaster Prep with regulatory inspections
c) Provides training and support for staff, parents and pupils raising awareness of e-Safety

d) Deputy Head (Prep):

a) Takes day-to-day responsibility for e-safety issues
b) Maintains incident logs of reported e-safety incidents
c) Maintains a Social Media Register and monitors the use of Social Media, reporting any incidents
d) Ensures that all staff, academic and non – academic are briefed on e-Safety responsibilities and procedures
e) Provides training and support for staff, parents and pupils raising awareness of e-Safety
f) Meets regularly with the e-Safety Governor, e-Safety co-ordinator (Senior) to discuss current status and to review incident logs

e) Head of IT Services:

a) Ensures that the ICT infrastructure is secure and is not open to misuse or malicious attack
b) Ensures that the accessibility of the network is enforced through a properly enforced password protection policy

c) Internet browsing is in line with the appropriate Filtering policy and that regular reports of suspicious activity are provided to the Principal Deputy Head (Senior School) and Deputy Head (Prep School)
d) Assists in the investigation of any misuse of the ICT systems supplied by the Trust. This may include the monitoring of email or files stored on the server in line with the Acceptable Use Policy

f) Teaching and Support Staff:

a) Read and digitally signed a copy of the "Staff Acceptable Use Policy and Guidelines", this should take place at the start of each academic year
b) Monitor the use of technology during lessons, activities, school events and trips which includes being aware of the use of pupils' mobile devices and social media in line with the "Pupils' Acceptable Use Policy and Guidelines"
c) Remain up to date and aware of e-safety matters
d) Embed e-safety elements throughout all aspects of the curriculum
e) Are familiar with reporting procedures for e-safety incidents
f) Use Social Media as stated in the "Staff Acceptable Use Policy and Guidelines" and give all necessary information to ensure the Social Media Register is up to date

g) Designated Safeguarding Lead:

a) Should be trained in e-safety specific incidents
b) Be familiar with the relevant procedures for reporting and handling incidents involving e-Safety elements
c) Provide clear guidance to staff with regards to the reporting and handling of Child Protection incidents

h) Pupil Voice and e-Safety committees:

Members of the Pupil Voice and School Council will assist the e-Safety Co-ordinators with:

a) The production and review of e-safety policy documents
b) Discussing and canvassing views from a range of pupil bodies (Day and Boarding)
c) The feedback of relevant information from discussions with pupils

i) Pupil Education:

a) A planned e-safety programme should be provided as part of ICT and Tutoring/ PSHE programme
b) Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
c) Key messages should be delivered across the Trust as part of Year Group, House and whole School assemblies

j) Staff Training:

a) A planned e-safety training session should be provided as part of the induction programme for all new staff at the beginning of the academic year
b) Updates as part of Child Protection Training will be given as whole or part of specific group (e.g. Housemaster) training
c) Key groups (e.g. House staff, Year Heads, SMT) will receive training or information during specific key meetings (e.g. weekly SMT, Housemaster or Year group meetings)
d) Summer School Induction is completed as part of Staff induction and is carried out by either the e-Safety Co-ordinator or an appointed member of the Summer School staff

k) Governor and Parent Communications and Training:

a) The education of Governors and Parents will be delivered by the e-Safety Co–ordinator in conjunction with the Head of IT Services and the Designated Safeguarding Leads on a regular basis, as a guide there should be communication and education on a termly basis.

l) Technical:

a) Passwords / Passphrases:

a) All users have clearly defined access rights to school ICT systems
b) All users have individual usernames and passwords which should be kept confidential
c) Users can only access data to which they have right of access
d) No user should be able to aces another's files, without permission (or as allowed for monitoring purposes as stated in this policy)

b) Filtering:

a) The internet feed is filtered in accordance with the specific user Filtering Policy

Owned by:	E-Safety Co-ordinator
Authorised by:	SMT
Date:	November 2018
Review Date:	November 2019
Circulation:	School website, All parents, All Staff, All Pupils

Appendix 1

Trust Incident Flow Chart

Considerations – risk assessment

- Vulnerability of the child
- Coercion
- How shared and where?
- Impact on the child
- Age of the child

Initial disclosure

This could come from a pupil directly, a parent, a pupil's friend.

Initial review with safeguarding team

Contact the DSL / the Principal Deputy / Deputy Head Prep immediately to review the information and consider the five points for immediate referral. They make an initial decision about whether the incident can be dealt with in house.

Risk assessment/Dealing with the incident

Consider the risk of harm and at any point if there are 'causes of concern' refer back to police/social care.

Management in school

Ensure parents are informed and the incident recorded following all child protection and safeguarding procedures.

Immediate referral:

1. Adult involvement
2. Coercion or blackmail
3. Extreme or violent
4. Under 13
5. Immediate risk of harm

Police/social care/MASH referral

Refer to your local arrangements for dealing with incidents and contact local services.

For further guidance visit:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609874/6_2939_SP_NCA_Sexting_In_Schools_FINAL_Update_Jan17.pdf