

# E-Safety Policy



Hydesville Tower  
School, Walsall

April 2017

---

## CONTENTS

### ESAFETY POLICY EXEMPLAR

Date created: January 2014 Reviewed: April 2016 Review: March 2017

By: J Warren Head of IT Curriculum

- 1.0 INTRODUCTION
- 2.0 WHOLE SCHOOL APPROACH
- 3.0 ACCEPTABLE USE OF TECHNOLOGY AGREEMENT AND REPORTING
- 4.0 STAFF AWARENESS AND TRAINING
- 5.0 E-SAFETY IN THE CURRICULUM
- 6.0 INFRASTRUCTURE AND DATA MANAGEMENT
- 7.0 MONITORING, AUDIT AND POLICY REVIEW
- INCIDENT REPORTING FORM

## 1.0 INTRODUCTION

1.1. This policy guidance is designed to guide your practice and policy writing for ensuring strong E-Safety procedures in your school. As a generic policy is not sufficient, you should use this document to draft a school specific policy with the inclusion of key stakeholders. This Exemplar has been drawn up with reference to current inspectorate guidance and advice of the CEOP and other E-Safety organisations. You should discuss each of its points with reference to your current policy and adapt as necessary to your school. It is recommended that your policy should follow this exemplar as closely as possible to ensure compliance.

1.2 We define E-Safety as:-

- ensuring student Internet use and access is appropriate and controlled.
- preventing misuse of Internet connected devices.
- ensuring students are educated on the risks carried with Internet use and how to minimise and deal with those risks.
- providing students with knowledge and resources to make decisions to ensure their safety online

1.3 Our core principles for E-Safety are:-

- The Internet and Internet connected devices provide a rich resource for supporting teaching and learning.
- Our policies seek to educate and inform students and the school community on the safe and prudent use of Internet resources
- We take a whole school, consistent approach to E-Safety, recognising that all staff should be involved and clear on their role in ensuring E-Safety education.
- E-Safety is subject to clear reporting routines and an age appropriate Acceptable Use of Technology Agreement is in place for all students.
- We recognise the need for regular training and ensure at least one member of staff takes accredited training and has a higher level of expertise.
- Our policy reflects current practice and is regularly reviewed and updated by the Lead Team and communicated to all staff.
- E-Safety is addressed within the curriculum at all ages.
- Technology in school is monitored to ensure it offers a safe access point to the Internet
- This policy should complement other school policies, in particular safeguarding policy; staff acceptable Internet and device use; data protection, anti-bullying or similar policies and student / pupil Acceptable Use of Technology Agreement.
- The E-Safety policy is dated with a review date and a named member of staff has responsibility for ensuring it is reviewed and updated on an annual basis

## 2.0 WHOLE SCHOOL APPROACH

2.1 We take a consistent approach to E-Safety and ensure that:

- All staff are aware of their responsibilities. E-Safety procedures are discussed in induction for new staff. The policy and procedures are discussed in staff briefings and training is provided at regular intervals.
- E-Safety is mentioned on the SDP noting current state of practice and any areas for development.
- We ensure all students understand what is meant by E-Safety through age appropriate delivery in the curriculum at all ages.
- All pupils are subject to the Acceptable Use of Technology Agreement (AUTA) which is signed by the students and discussed at the start of each new academic year.
- Parents are aware of their children's responsibilities under the AUTA and sign the agreement for younger students/ pupils.
- Awareness raising events are held, such as assemblies, parents' forums and PSCO visits.
- E-Safety is raised as part of school council discussions
- There are notices and posters giving guidance on display in key areas of the school.

## 3.0 ACCEPTABLE USE OF TECHNOLOGY AGREEMENT AND REPORTING

3.1 We hold an Acceptable Use of Technology Agreement (AUTA) that sets out positive guidelines for how students should use and treat technology both during the school day and outside school as school representatives.

3.2 The AUTA is delivered to all students with a discussion of the points at the beginning of the academic year. The agreement is adapted to the age of the students and older students are expected to sign the agreement. The agreement is presented to students joining the school outside of the start of the academic year.

3.3. The AUTA sets out guidelines for:

- appropriate and respectful use of school technology equipment and devices
- expectations and regulations for the use of students own devices in school
- expectations of behaviour if equipment is found broken or non-functional
- appropriate communications using devices in and out of school
- code of practice if students discover inappropriate or upsetting material on any device
- clear guidance on how to report any concerns

3.4 The AUTA is used positively to encourage appropriate and E-Safe behaviour and can be used alongside rewards for positive use of technology

3.5. The AUTA is supported by a clear set of age appropriate sanctions for behaviour that contradicts the agreement. Sanctions at each level should be recorded and a member of the Lead Team should be made aware of any sanctions applied to students. Records of any behaviour outside the agreement should be held, with clear description of the incident and sanctions applied

3.6 The AUTA is shared with parents and their views are welcomed and considered.

3.7 The AUTA is not intended to form the whole basis of E-Safety education, but to complement discussions and lessons on E-Safety during curriculum time and to provide a robust agreement setting out clear expectations for behaviour

3.8 The AUTA is designed to be binding for students while *enrolled* in the school and the school reserves the right to take action on behaviour that contradicts the Agreement outside of school time. In these cases the school will proceed with discretion and in partnership with parents.

3.9 Students, parents and all staff are able to report concerns and guidance for this should be set out in the AUTA

---

### ESAFETY POLICY EXEMPLAR

Date created: January 2014 Reviewed: April 2016 Review: March 2017

By: J Warren Head of IT Curriculum

## 4.0 STAFF AWARENESS AND TRAINING

4.1 All staff are bound by the code of practice set out in the Cognita Schools Policy for use of Internet and mobile devices. This should be available for all staff and ensures that staff use technology safely and with adherence to safeguarding principles.

4.2 At least one member of staff should undertake accredited training. We recommend the Keeping Children Safe Online (KCSO) course provided by the CEOP. *This training is delivered online and is suggested to take 3 hours in total although it is not necessary for the course to be taken in one 'sitting'.*

4.3 The accredited member of staff should provide a higher level of expertise within the school and can guide staff in E-Safety practice and review of E-Safety policy and procedure and provide INSET guidance

4.4 E-Safety should be built into the termly programme of meetings to ensure all staff are aware of their responsibilities and for the discussion of any issues, concerns or opportunities for events or cross curricular E-Safety lessons.

4.5. There should be a clear procedure for staff wishing to report or discuss concerns relating to E-Safety or Internet access in the school. This procedure should include reporting to a member of Lead Team should be documented as necessary.

4.6 Staff responsibilities for E-Safety are: (for all staff)

- To ensure they are familiar with and fully support the student Acceptable Use of Technology Agreement
- To be vigilant when using technology as part of lessons
- To model safe and responsible use of school technology
- To provide reminders and guidance to students on acceptable use
- To report and act appropriately if they become aware of, or after any student reports, a concern or an incident involving technology use
- To ensure E-Safety is delivered within the curriculum as appropriate to their student age range and subject area
- To contribute to and discuss E-Safety policy and to have their views heard
- To be aware of the school policy for tackling bullying and how this relates to incidents of cyber-bullying
- To be mindful of protecting data and keeping access to digital information secure by adhering to the school password policy and protecting their accounts from student access.
- To use secure portable data options including password protected or encrypted portable memory devices

## 5.0 E-SAFETY IN THE CURRICULUM

5.1 E-Safety should be embedded into the curriculum at all age ranges. Lessons should be well planned and resourced and there should be a number of opportunities to discuss a range of E-Safety issues.

5.2 E-Safety is expected to be covered within ICT and PSHE lessons but should not be exclusive to these subject areas and discussion of E-Safety should be explored in other subject areas both while using technology and as a topic as appropriate

5.3 Guidance on minimum coverage in each key stage:-

EYFS – safe and responsible use of technology should be modelled; Suggestions relating to ELG could include:

Communication and Language – pupils aware that they are able to communicate with others using devices – appropriate language and key words associated with technology

Physical development – safe and careful handling of technology

Personal, Social and Emotional development – sharing and cooperating while using technology

---

### ESAFETY POLICY EXEMPLAR

Date created: January 2014 Reviewed: April 2016 Review: March 2017

By: J Warren Head of IT Curriculum

Understanding of the World – awareness of devices around us and how they are used to keep us safe, provide us with information

EYFS children should be given opportunities to learn collaboratively with devices

Key Stage 1 – Typical KS1 E-Safety coverage should address: Pupils should be made aware of distinction between personal, private and public information. Pupils should be taught appropriate ways to communicate when using devices and how to respond to unpleasant or distressing comments they may encounter online. They should be made aware that people they do not know are strangers including while playing online games and the importance of using ‘usernames’ and guarding against volunteering information. They should be taught how to respond if they are distressed or uncertain about any material they are exposed to while online or using technology.

Key Stage 2 – Issues outlined above should be addressed with the addition of: Importance of passwords and cyber security. Understanding of how cyberbullying is using technology to be unpleasant and guidance on how to respond constructively and report any thing that concerns them. Understanding of how social networks allow sharing of information and the importance of keeping information about themselves private. Understanding of how data submitted to the Internet including photographs, comments, emails etc. can be potentially accessed, altered and used by anyone. Clearer understanding of distinction between private and public information. Discussion of support networks and methods of reporting anything they are uncertain or concerned about. Understanding of spam, unsolicited and scam activity on the Internet and how accounts can be hacked or accessed by criminals.

Key Stage 3 and 4– Issues outlined above are all relevant with the addition of: Discussion of E-Safety issues in the news and current affairs. Understanding of the law and relevant acts passed to protect people from discrimination, abuse and exposure to indecent content. Discussion of how photographs, information and comments posted online can be accessed by any one and cannot be retracted or removed easily. Fuller understanding of how everyday use of technology can be made more secure through intelligent password use, vigilance and due care when using public technology facilities. Understanding of plagiarism and copyright laws. Addictive nature of devices. Access to relevant support networks and guidance on dealing with cyberbullying, peer pressure and social aspects of device use.

5.4 Extra –curricular activities such as Safer Internet Day opportunities, visits from local PSCO, school assemblies should be explored but these should not represent the majority of E-Safety teaching or discussion in the academic year. They should be used to support lessons embedded in the curriculum.

5.5 Use of mobile devices during lessons is subject to control and risk management.

Expectations of appropriate use of mobile devices are set out in the AUTA for students. This includes students are expected not to share digital images or videos of other students taken during lessons for any purpose other than school use.

5.5 Opportunities for peer mentoring or ‘buddy’ systems can be explored so that older pupils can act as role models for younger children and provide a further method for students to report concerns

## **6.0 INFRASTRUCTURE AND DATA MANAGEMENT**

6.1 The school Internet access is subject to filtering and control and this is updated regularly

6.2 Staff are aware of how to use safe-searching options and are vigilant during lessons involving Internet access

6.3 Where available, screen watching facilities are used and staff are aware of how to utilise these resources

6.4 Passwords and digital security is in place to protect data and data is managed in accordance with the relevant DP Acts

6.5 Staff are fully aware of how to report a problem or any incidents relating to data security or Internet control

6.6 Professional communications between the school and other organisations or parents take place within clear professional boundaries, are transparent and open to scrutiny and do not share personal information with students

## **7.0 MONITORING, AUDIT AND POLICY REVIEW**

7.1 The E-Safety policy is dated and an annual review date is stated with a named member of staff responsible for ensuring it is reviewed and updated

7.2 It may be necessary for more frequent reviews if a number of incidents are recorded.

7.3 The review procedure should be:

- An audit of effectiveness of current practice
- A review of guidance published by relevant organisations
- Amendments to be shared with all staff

7.4 To audit E-Safety effectiveness of the current policy the following questions should be considered:

- Has recording of E-Safety incidents been effective – are records kept?
- Did the school feel able to respond effectively to any incidents?
- Were incidents resolved to the best of the school's ability?
- Do all students demonstrate an awareness of E-Safety appropriate to their age?
- Have complaints or concerns with the policy been recorded and addressed?
- Have there been significant developments in technology that should be addressed either within the curriculum or as part of staff awareness training?
- Is the policy clear to all staff and seen as appropriate and working?
- Is the current wording of the Acceptable Use of Technology Agreement fit for purpose and reflective of technology use in the school?
- Do all members of the school community know how to report a problem?
- Is E-Safety observed in teaching and present in curriculum planning documents?

Incident Reporting form exemplar

<b><u>Breach of the Acceptable Use of Technology Agreement</u></b> <b><u>Report of Incident Form</u></b>	
Date:	
Date(s) of incident(s):	
Staff member completing form:	
Further staff members dealing with incident:	
Name of student(s) involved:	
Parents informed:	
Location of incident:	
Name of IT Team member informed:	
Please give details of the incident:	
Please give details of sanctions applied / action taken	
Is any follow up action required (additional eSafety lessons, invited speakers, referral etc.)?	
Signed: staff member	
Signed ESafety lead:	