



E-safety Policy

2017-2020

Adopted by Symphony Learning Trust on	Spring 2017
Next Review Due	Spring 2020

For the purpose of this policy, the 'Head teacher' refers to the Executive Head teacher, Head teacher or Head of School.



E-SAFETY POLICY

- 1. Introduction**
- 2. Scope of Policy**
- 3. Policies and Practices**
 - 3.1 Use of internet facilities, mobile and digital technologies**
 - 3.2 Reporting abuse**
- 4. Education and Training**
- 5. Infrastructure and Technology**
 - 5.1 Partnership working**
- 6. Inspection and Standards**
 - 6.1 Monitoring**
 - 6.2 Sanctions**
- 7. Working in partnership with Parents and Carers**

- 1. Introduction**



1.1 The schools in Symphony Learning Trust recognise the internet and other digital technologies provide a vast opportunity for children and young people to learn. Unlike any other mode of technology, the internet and digital technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.

1.2 As part of our commitment to learning and achievement we want to ensure that the internet and other digital technologies are used to:

- Raise educational standards and promote pupil achievement.
- Develop the curriculum and make learning exciting and purposeful.
- Enable pupils to gain access to a wide span of knowledge in a way that ensures their safety and security.

To enable this to happen we have taken a whole school approach to E-safety which includes the development of policies and practices, the education and training of staff and pupils and the effective use of the School's infrastructure and technologies.

1.3The schools in Symphony Learning Trust as part of this policy holds steadfastly to the ethos that there should be an equitable learning experience for all pupils using technology. We recognise that technology can allow disabled pupils increased access to the curriculum and other aspects related to learning.

1.4 The schools in Symphony Learning Trust are committed to ensuring that **all** its pupils will be able to use existing, as well as up and coming technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents, are educated as to the dangers that exist so that they can take an active part in safeguarding them.

1.5The nominated senior person for the implementation of the School's E- safety policy is the Head Teacher

2. Scope of Policy

2.1The policy applies to:



- all pupils;
- all teaching and support staff (including peripatetic), school governors and volunteers;
- all aspects of the School's facilities where they are used by voluntary, statutory or community organisations.

2.2 The schools in Symphony Learning Trust will ensure that the following elements are in place as part of its safeguarding responsibilities to pupils:

- a list of authorised persons who have various responsibilities for E-safety;
- a range of policies including acceptable use policies that are frequently reviewed and updated;
- information to parents that highlights safe practice for children and young people when using the internet and other digital technologies;
- adequate training for staff and volunteers;
- adequate supervision of pupils when using the internet and digital technologies;
- education that is aimed at ensuring safe use of internet and digital technologies;
- a reporting procedure for abuse and misuse.

3. Policies and Procedures

The schools in Symphony Learning Trust understand that effective policies and procedures are the backbone to developing a whole-school approach to E-safety. The policies that exist at the schools in Symphony Learning Trust are aimed at providing a balance between exploring the educational potential of new technologies and providing safeguards to pupils.

3.1 Use of internet facilities, mobile and digital technologies

3.1.1. The schools in Symphony Learning Trust will seek to ensure that internet, mobile and digital technologies are used effectively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk.

3.1.2 The schools in Symphony Learning Trust expect all staff and pupils to use the internet, mobile and digital technologies responsibly and strictly according to the conditions below. These expectations are also applicable to any voluntary, statutory



and community organisations that makes use of the school's ICT facilities and digital technologies.

Users shall not:

- Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
 - Indecent images of children
 - Promoting discrimination of any kind
 - Promoting racial or religious hatred
 - Promoting illegal acts
 - Any other information which may be offensive to peers or colleagues.

3.1.3 The schools in Symphony Learning Trust recognise that in certain planned curricular activities, access to otherwise deemed inappropriate sites may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned and recorded so that it can be justified if required.

3.1.4 Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the Police:

Images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative)

- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist or anti-religious material
- Violence and bomb making
- Illegal taking or promotion of drugs
- Software piracy
- Other criminal activity

3.1.5 In addition, users may not:

- Use the broadband provider's facilities for running a private business;
- Enter into any personal transaction that involves the school or associated partners in any way;
- Visit sites that might be defamatory or incur liability on the part of the school or associated partners or adversely impact on the image of the school or associated partners;



- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties;
- Reveal or publicise confidential or proprietary information, which includes but is not limited to:
 - financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships;
 - Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet;
 - Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate.
 - Transmit unsolicited commercial or advertising material either to other user organisations or to organisations connected to other networks, save where the material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe.
- Assist with unauthorized access to facilities or services
- Undertake activities with any of the following characteristics:
 - wasting staff effort or networked resources, including time on end systems accessible via the network and the effort of staff involved in support of those systems;
 - corrupting or destroying other users' data;
 - violating the privacy of other users;
 - disrupting the work of other users;
 - using the network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
 - continuing to use an item of networking software or hardware after request that use cease because it is causing disruption to the correct functioning of the network;
 - other misuse of the network, such as introduction of viruses.
- Use mobile technologies (e.g. 4G, 3G or mobile internet services) in any way to intimidate, threaten or cause harm to others. Moreover, mobile technologies should not be used to access inappropriate materials or encourage activities that are dangerous or illegal.

3.2 Reporting Abuse



The following outlines what to do if a child or adult receives an abusive message or accidentally accesses a website that contains abusive material:

The abusive material should be stored, screenshot if possible and a copy sent to the headteacher of the school. The address (e.g. URL or email) linked to the abuse should also be recorded. However, the screen displaying the abusive material should be hidden from view and/or closed down as soon as possible to avoid further offence. The E-safety Incident/Concern Form should be filled out alongside this and given to the headteacher as soon as possible.

4. Education and Training

4.1 The schools in Symphony Learning Trust recognise that the internet and other digital technologies can transform learning; help to improve outcomes for children and young people; promote creativity; all of which add up to a more exciting and challenging classroom experience.

4.2 As part of achieving this, we want to create within each school an accessible system, with information and services online, which support personalised learning and choice. However, we realise that it will be necessary for our pupils to have the skills of critical awareness, digital literacy and good online citizenship to enable them to use the internet and other digital technologies safely.

4.3 To this end, the schools in Symphony Learning Trust will:-

- Enable all pupils to exercise the skills of critical awareness, digital literacy and good online citizenship as part of the school curriculum.
- Educate school staff so that they are equipped to support pupils in gaining positive experiences when online and can help pupils develop strategies if they encounter a problem.
- Support parents in gaining an appreciation of E-safety for their children and provide them with relevant information on the policies and procedures that govern the use of internet and other digital technologies within the school.

5. Infrastructure and Technology

5.1 Partnership working

5.1.1 The schools in Symphony Learning Trust recognise that as part of its safeguarding responsibilities there is a need to work in partnership. One of our major partners is the network and broadband supplier. As part of our commitment to partnership working, we fully support and will continue to work with our providers to ensure that pupil and staff usage of the internet and digital technologies is safe.

5.1.2 The schools in Symphony Learning Trust will, as part of its wider safeguarding responsibilities, seek to ensure that voluntary, statutory and community organisation take an approach to their activities that see the welfare of the child as paramount. To this end, we expect any organisation using the school's ICT or digital technologies



to have appropriate policies and procedures that are aimed at safeguarding children and young people and reporting concerns.

6. Standards and Inspection

The schools in Symphony Learning Trust recognise the need to have regular inspections of policies and procedures in order to ensure that its practices are effective and that the risks to pupils are minimised.

6.1 Monitoring

6.1.1 Monitoring the safe use of the internet and other digital technologies goes beyond the personal use of the internet and electronic mail a pupil or member of staff may have, the schools in Symphony Learning Trust recognise that in order to develop an effective whole school E-safety approach there is a need to monitor patterns and trends of use inside school and outside school (Education and Inspections Act 2006, Section 89(5)).

6.1.2 With regard to monitoring trends, within the school and individual use by school staff and pupils, the schools in Symphony Learning Trust will audit the use of the internet and electronic mail in order to ensure compliance with this policy. The school will also work with its internet service provider to further ensure compliance.

6.1.3 Another aspect of monitoring, which our school will employ, is the use of mobile technologies by pupils, particularly where these technologies may be used to cause harm to others, e.g. bullying (see anti-bullying policy for further information). We will also ensure that school staff understand the need to monitor our pupils, and where necessary, support individual pupils where they have been deliberately or inadvertently been subject to harm.

6.2 Sanctions

6.2.1 The schools in Symphony Learning Trust has been careful to develop in conjunction with its partners, policies and procedures to support the innocent in the event of a policy breach and enable the School to manage such situations in, and with, confidence.

6.2.2 Where there is inappropriate or illegal use of the internet and digital technologies, the following sanctions will be applied:

Child / Young Person

- The child/young person will be disciplined according to the behaviour policy of the school, which could ultimately include the use of internet and digital technologies being withdrawn.



- Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

Adult (Staff and Volunteers)

- The adult may be subject to the disciplinary process, if it is deemed he/she has breached the policy
- Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

6.2.3 If inappropriate material is accessed, users are required to immediately report this to the headteacher so this can be taken into account for monitoring purposes.

7. Working in Partnership with Parents and Carers

7.1 The schools in Symphony Learning Trust are committed to working in partnership with parents and carers and understand the key role they play in the E-safety of their children, through promoting E-safety at home and elsewhere.

7.2 The schools in Symphony Learning Trust also appreciate that there may be some parents and carers who are concerned about the use of the internet, email and other digital technologies in school. In such circumstances school staff will meet with parents and carers to discuss their concerns and agree upon a series of alternatives that will allow their child to fully access the curriculum, whilst remaining safe.

8. Appendices of the E-safety Policy

8.1 There are multiple aspects of the school's E-safety policy, which include acceptable use policies for both staff and pupils; ICT equipment (onsite and offsite); data security and retention. The various policy documents relating to these aspects of the school's E-safety policy can be obtained from the headteacher for scrutiny, if required.



E- Safety Incident/Concern Form

Please complete as soon as possible and return to the designated person

School name..... Designated Senior Leader.....

Name of child:		Age of child:	
Date /time/ place (home or school) of concern:			
Nature of concern/incident:			
Evidence (e.g text, email, print out or screenshot) Is the evidence still available?			
Reported by: Designation			
Other witnesses: Pupils Adults			
Reported to(please name)			
Signed:	Witness		
Signed:	Designated Senior Leader		
Action (to be completed by designated leader			
Outcome (to be completed by designated person)			