# E-SAFETY POLICY

DATE AGREED: SEPTEMBER 2017
REVIEW DATE: SEPTEMBER 2019

## 1. Introduction

At Swallowdale we recognise the crucial role the internet and other technologies have in preparing our children for the digital age that they live in. We understand the important role that technology can play in enhancing teaching and learning through promoting creativity, stimulating awareness and developing life skills allowing our children to fly high. It is our goal to deliver an integrated computing curriculum which raises educational standards in all subjects whilst providing equal opportunities for every pupil.

Swallowdale's fundamental concern is the safety of our children. We follow advice from the U.K Council for Child Internet Safety (UKCCIS) which is used in the development of policy and in the training of staff and pupils to use the school's technology appropriately. Following local authority guidelines, we are committed to ensuring that all those who work with children and young people, including their parents, are properly educated and informed about associated risks.

## 2. Roles and Responsibilities

The Headteacher is responsible for ensuring the safety (including e-safety) of all members of the school community.

The e-safety Leader will work with the Headteacher and the designated Child Protection Coordinators, to have an overview of the serious child protection issues that arise from sharing of personal data, access to illegal or inappropriate materials, inappropriate online contact with adults, potential or actual incidents of grooming and cyber-bullying.

| Role | Responsibility |
|---|---|
| **Governors** | • Approve and review the effectiveness of the e-safety Policy<br>.<br>• Will ensure this policy complements and supports our Safeguarding/Child Protection Policy.<br><br>• Delegate a governor to act as e-safety link |

| | |
|---|---|
| | • e-safety Governor works with the e-safety Leader to carry out regular monitoring and report to Governors |
| **Head Teacher and Senior Leaders** | • Ensure that all staff receive suitable CPD to carry out their e-safety roles<br>• Create a culture where staff and learners feel able to report incidents<br>• Ensure that there is a progressive e-safety curriculum in place<br>• Ensure that there is a system in place for monitoring e-safety<br>• Follow correct procedure in the event of a serious e-safety allegation being made against a member of staff or pupil<br>• Inform the local authority about any serious e-safety issues<br>• Ensure that the school infrastructure/network is as safe and secure as possible<br>• Ensure that policies and procedures approved within this policy are implemented<br>• Use an audit to annually review e-safety with the school's technical support |
| **e-safety Leader** | • Lead the e-safety working group<br>• Log, manage and inform others of e-safety incidents and how they have been resolved where this is appropriate<br>• Lead the establishment and review of e-safety policies and documents<br>• Lead and monitor a progressive e-safety curriculum for pupils<br>• Ensure all staff are aware of the procedures outlined in policies relating to e-safety |

| | |
|---|---|
| | • Provide and/or broker training and advice for staff<br>• Attend updates and liaise with the LA e-safety staff and technical staff<br>• Meet with Senior Leadership Team and e-safety Governor to regularly discuss incidents and developments<br>• Coordinate work with the school's designated Child Protection Coordinator |
| Teaching and Support Staff | • Participate in any training and awareness raising sessions<br>• Read, understand and sign the Staff AUP<br>• Act in accordance with the AUP and e-safety Policy<br>• Report any suspected misuse or concerns to the e-safety Leader and check this has been recorded<br>• Provide appropriate e-safety learning opportunities as part of a progressive e-safety curriculum and respond<br>• Model the safe use of technology<br>• Monitor ICT activity in lessons, extracurricular and extended school activities<br>• Demonstrate consistently high standards of personal and professional conduct especially in relation to use of social networks, making sure that these are in line with school ethos and policies, including at the time of a Critical Incident.<br>• Share policy with staff. |
| Pupils | • Read, understand and sign the Pupil AUP and the agreed class Internet rules<br>• Participate in e-safety activities, follow the AUP and report concerns for themselves or others<br>• Understand that the e-safety Policy covers actions out of school that are related to their membership of the school |
| Parents | • Endorse (by signature) the Pupil AUP |

| | |
|---|---|
| and Carers | • Discuss e-safety issues with their child(ren) and monitor their home use of technology (including tablets, mobile phones and games devices) and the Internet<br>• Access the school website in accordance with the relevant school AUP<br>• Keep up to date with issues through newsletters and other opportunities<br>• Inform the Headteacher of any e-safety issues that relate to the school<br>• Maintain responsible standards when using social media to discuss school issues<br>• Subscription to Parent Zone magazine. |
| Technical Support Provider | • Ensure the school's ICT infrastructure is as secure as possible and is protected from misuse or malicious attack<br>• Ensure users may only access the school network through an enforced password protection policy<br>• Maintain and inform the Senior Leadership Team of issues relating to filtering<br>• Keep up to date with e-safety technical information and update others as relevant<br>• Ensure use of the network is regularly monitored in order that any misuse can be reported to the e-safety Leader for investigation<br>• Ensure monitoring systems are implemented and updated<br>• Ensure all security updates are applied (including anti-virus and Windows) |
| Community | • Sign and follow the Guest/Staff AUP before being provided with access to school systems |

## 3. Scope of Policy

This 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.

Swallowdale 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;
- training for staff and volunteers;
- 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.

## 4. Education of pupil

A progressive planned e-safety education programme takes place through discrete lessons and across the curriculum, for all children in all years, and is regularly revisited.

- key e-safety messages are reinforced through assemblies, Safer Internet Week (February), anti-bullying week (November) and throughout all lessons

- pupils are taught to keep themselves safe online and to be responsible in their use of different technologies.

- pupils are guided to use age appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material

- in lessons where Internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in Internet searches

- pupils are taught to be critically aware of the content they access online and are guided to validate the accuracy and reliability of information

- pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet

- pupils are taught about current issues such as online gaming, extremism, vlogging and obsessive use of technology

- pupils will write and sign an AUP for their class at the beginning of each school year, which will be shared with parents and carers

- pupils are educated to recognise and respond appropriately to 'different forms of bullying, including cyber-bullying'

## 5. Education for parents

Parents and carers will be informed about the ways the Internet and technology is used in school. They have a critical role to play in supporting their children with managing e-safety risks at home, reinforcing key messages about e-safety and regulating their home experiences. The school supports parents and carers to do this by:

- providing clear AUP guidance which they are asked to sign with their children and regular newsletter and website updates;

- raising awareness through activities planned by pupils;

- inviting parents to attend activities such as e-safety week, e-safety assemblies or other meetings as appropriate;

- providing and maintaining links to up to date information on the school website

## 6. Training of staff

There is a planned programme of e-safety training for all staff and governors to ensure they understand their responsibilities, as outlined in this, and the AUPs. This includes:

- an annual audit of the e-safety training needs of **all** staff

- **all** new staff and governors receiving e-safety training as part of their induction programme

- providing information to supply and student teachers on the school's e-safety procedures

- this e-safety Policy and its updates being shared and discussed in staff meetings and in Governor meetings

- the e-safety Leader providing guidance and training as required to individuals and seeking LA support on issues

- staff and governors are made aware of the UK Safer Internet Centre helpline 0844 381 4772

## 7. Infrastructure and Technology

At Swallowdale we recognise the need to work in partnership with external parties to enhance the safety of our children and staff. We work with East Midlands Broadband Community (embc) who provide our network and alongside Capita's openhive system ensure that our internet provision is filtered and secure. Additionally, we use the services of Systems for Education to maintain the integrity and functionality of the school's hardware and server.

As part of our commitment to protecting our children and adults, we endeavour to ensure that any external party working with our school have appropriate policies and procedures for safeguarding children and young people.

## 8. Policy and procedures

**Use of internet, mobile and digital technologies**

- Technology should be used effectively for their intended educational purpose without infringing legal requirements or creating unnecessary risk.
- All adults and pupils using the internet, mobile and digital technologies should use them responsibly and follow the conditions listed below.

Users should **not**:

- Visit internet sites, make, post, download, upload or pass on any material, remarks, proposals or comments that contain or relate to:
    - Indecent images of children
    - Promoting discrimination
    - Promoting racial or religious hatred
    - Promoting illegal acts
    - Any other material which may be considered offensive to peers and colleagues.
- Swallowdale recognises that at times access to sites blocked by the school's filtering system might be necessary to allow the delivery of the curriculum. Access to such materials should be first approved by the e-safety coordinator/ computing coordinator and then reported to a member of the senior management team so an accurate record can be kept.

- Incidents where inappropriate material has been accessed by any individual in school should be immediately reported the headteacher and logged in the e-safety log. The headteacher, based on the nature of the material accessed and in consultation with UKCCIS and local authority guidelines will then decide the most appropriate course of action to take.

- Individuals should be aware that if our external parties (embc, Capita or Systems for Education) become aware of illegal activity they will take action directly and inform the police.

- In the event of a supply teacher being used in school, the account supply should be used. Before its use the individual should be asked to sign the school's acceptable use policy for staff.

- Staff, pupils and other adults should not use the computing facilities provided by Swallowdale Primary School to:
    - run a private business
    - carry out any personal financial transactions
    - use commercial software which may infringe copyright laws
    - Interfere with the school network (including the propagation of computer viruses or causing network congestion through the upload and download of data irrelevant to the individual's profession job).
    - Use Swallowdale's internet or hardware for the representation of personal opinion or revealing confidential information.
    - Assist individuals to access facilities which are unauthorised through embc and openhive.
    - Tamper with another individual's work.
    - Installing software without specific permission.

- As is best practice, staff are required to use a password for any encrypted device which is secure. This password should be changed every half term. Passwords should never be shared with anyone other than the computing coordinator or technician and even then should be immediately changed.

- Staff are required to allow anti-virus updates to take place on their machines. Only messages from our Panda anti-virus software should be accepted.

## 9. Policy on Cyberbullying

Peer-on-peer abuse is any form of physical, sexual, emotional and coercive control, exercised between children and within children's relationships (both intimate and non-intimate). Peer-on-peer abuse can take various forms, including: serious bullying (including **cyber-bullying),** relationship abuse, domestic violence, child sexual exploitation, youth and serious youth violence, harmful sexual behaviour, and/or genderbased violence.

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated.

The school will follow procedures in place to support anyone in the school community affected by cyberbullying.

Pupils and staff are made aware of a range of ways of reporting concerns about cyberbullying e.g. telling a trusted adult or Childline Phone number 0800 1111.

Pupils, staff and parents and carers will be encouraged to report any incidents of cyberbullying and advised to keep electronic evidence.

All incidents of cyberbullying reported to the school will be recorded by the school.

The school will follow procedures to investigate incidents or allegations of cyberbullying.

The school will take steps where possible and appropriate, to identify the bully. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police.

Pupils, staff and parents and carers will be required to work with the school to support the approach to cyberbullying and the school's e-safety ethos.

Sanctions for those involved in cyberbullying will follow those for other bullying incidents and may include:

- the bully being asked to remove any material deemed to be inappropriate or the service provider being contacted to remove content if the bully refuses or is unable to delete content

- Internet access being suspended at the school for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or AUP

- the parent and carers of pupils being informed

- the police being contacted if a criminal offence is suspected

## 10. Policy on use of digital and video images

Photographs and video taken within school are used to support learning experiences across the curriculum, to share learning with parents and carers on our school's learning platform and to provide information about the school on the website. The school will:

- when using digital images, instruct staff to educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites
- allow staff to take images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images
- make sure that images or videos that include pupils will be selected carefully with their knowledge
- seek permission from parents or carers before images or videos of pupils are electronically published
- Encourage pupils to seek permission from other pupils to take, use, share, publish or distribute images of them without their permission
- all parties must recognise that any published image could be reused and repurposed
- make sure that pupils' full names will not be used anywhere on the school website, particularly in association with photographs, unless permission has been given in advance
- not publish pupils' work without their permission and the permission of their parents
- keep the written consent where pupils' images are used for publicity purposes, until the image is no longer in use

## 11. Data Protection Policy

The school will do everything possible so that the requirements in relation to the Data Protection Act 1998 are met.

The school will:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- use personal data only on secure password protected computers and other devices

- ensure that users are properly ‘logged-off’ at the end of any session in which they are accessing personal data

- store or transfer data using approved services such as encrypted and secure password protected devices

- make sure data is deleted from the device it has been transferred or its use is complete