



## Online Safety Policy Document

### Shawclough Community Primary School

Manager: S Clegg and Computing

Reviewed: June 2022  
Approved by Governors: May 2022  
Next Review: June 2023

#### Acknowledgments

This policy was adapted from the Archibald First School policy

#### ONLINE SAFETY POLICY

The school's online safety policy will operate in conjunction with other school policies including those for behaviour, PSHCE, safeguarding and photographs and will be reviewed every 3 years. It also operates in line with *Keeping Children Safe in Education September 2020* – in relation to online safety whilst homelearning.

#### Why we need this policy

New technologies have revolutionised the movement, access, and storage of information with important implications for all schools. Use of ever more powerful computers, broadcast media, the Internet, digital recorders of sound and images together with increased opportunities to collaborate and communicate are changing established ideas of when and where learning takes place. At Shawclough Community Primary School, we recognise that learning is a lifelong process and that e-learning is an integral part of it. Ensuring that we provide pupils with the skills to make the most of information and communication technologies is an essential part of our curriculum. The school is committed to the continuing development of our Computing infrastructure and embracing new technologies so as to maximise the opportunities for all pupils, staff, parents and the wider community to engage in productive, cooperative and efficient communication and information sharing.

However, as in any other area of life, children are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. Additionally, some young people may find themselves involved in activities which are inappropriate, or possibly illegal. Online Safety seeks to address the issues around using these technologies safely and promote an awareness of the benefits and the risks.

This policy sets out clearly our expectations on pupils, staff, parents and members of the wider community to ensure best practice.

## Contents

- Roles and Responsibilities
- What is Online Safety?
- Communications Policy
- Teaching and Learning
- The Internet – Why internet use is important, Authorising internet access, community use of the internet, bullying
- Internet safety
- Network safety
- Managing Internet
- Email
- School website
- Social networking
- Sexting
- Electronic Communications – mobile phones and digital cameras.
- Acceptable use for staff
- Acceptable use for pupils
- Copyright
- Data protection & protecting personal data
- Physical safety
- Esafety contacts & references
- Disclaimer
- Disposal of equipment

### ROLES AND RESPONSIBILITIES

The Headteacher of Shawclough Community Primary School (who is the Designated Senior Member of Staff for Online Safety) will ensure that:

- All staff should be included in Online Safety training. Staff must also understand that misuse of the internet may lead to disciplinary action and possible dismissal.
- All temporary staff and volunteers are made aware of the School's Online Safety Policy and arrangements.
- A commitment to Online safety is an integral part of the safer recruitment and selection process of staff and volunteers.
- The Headteacher is the first point of contact with regards to breaches in online safety and security.
- The headteacher will liaise with the Designated Person for Safeguarding as appropriate.
- IT security is maintained.
- appropriate training is attended.

The Headteacher or, in her absence, the Deputy Headteachers or next member of the School Leadership Team, has the ultimate responsibility for safeguarding and promoting the welfare of pupils in their care.

### What is Online-safety?

Online Safety encompasses the use of Internet technologies and electronic communications such as webcams, digital video equipment, mobile phones, camera phones, i-pods, i-pads and portable media players. It highlights the need to educate pupils about the benefits, risks and responsibilities of using information technology as well as raising user's awareness of how to keep themselves safe using electronic technology.

Shawclough Community Primary School will provide a framework for safe and appropriate use of

the Internet and other technology, this framework also extends to homelearning. As a school we aim to create a safe IT learning environment for the whole school community and to balance fulfilling the need to give pupils full access to resources with the need to protect them from unacceptable materials.

## Communications Policy

The Online Safety and Acceptable Use Policy will be thoroughly introduced to all staff, pupils and parents and its importance explained. All staff and other users are required to follow the conditions laid down in the policy. Users will be informed that Internet use is carefully monitored and that actions can be traced to an individual user. Staff should use IT resources discretely and professionally. In the case of employees breach of the conditions may constitute a breach of conditions of service and could lead to dismissal on the grounds of misconduct.

In the case of pupils breaching the conditions the following sanctions may be enforced:

- Temporary or permanent ban on Internet use.
- Additional disciplinary action in line with school behaviour policies
- Parents and other external agencies may be contacted.

The Online Safety rules (Appendix 1) will be visible by all computers.

## Teaching and Learning

Computing in schools is taught as a subject in its own right and also supports children's learning in and across the entire curriculum. Within Computing lessons children learn to use a wide range of IT resources including Internet, email, blogging, coding, i-pad, i-pods and digital cameras.

To ensure, that we keep abreast of new developments and technology, we have a Computing Team who provide support for others and drive the Computing Curriculum within school. The team consists of the following:

- Stuart Clegg
- Kay Collins
- Clare Fleming

See also the Computing Policy

## The Internet

### Why Internet use is important?

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. The Internet gives staff and pupils access to a global network of information, including:

- A wider range of resources and materials which can enrich subject learning across all curriculum areas, as well as independent study and cross curricular project work.
- Opportunities for world-wide communication with other pupils and teachers.
- Opportunities for the development of independent learning and research skills.
- Cultural, social and leisure information.
- A range of support services.

In addition, it can lead to:

- Development of network literacy (i.e. the capacity to use electronic networks to access resources, create resources and communicate with others - these can be seen as complex extensions of the traditional skills of reading, writing, speaking and listening, awareness of audience);
- Social development.

The school Internet access will be designed expressly for pupils and will include filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils. All pupils will be taught the '5 smart rules' from Childnet International. The rules will be

on display throughout the school – children will be reminded about safe use of internet whilst involved in any home learning.

Older pupils will also be taught how to evaluate Internet content as materials on the Internet vary hugely in quality: some materials are biased, inaccurate or misleading, either deliberately or unintentionally. Internet users will be taught the need to be aware of these issues and the need to exercise caution and judgement in their use of any material they find. The school will ensure that copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law. Downloading of files is restricted to staff, or pupils under supervision.

#### **Authorising Internet access**

- All staff must read and sign the 'Policy for employing use of email, the internet and Rochdale's intranet policy' before using any school IT resource. (see Appendix 2)
- Parents and children must read and sign the age appropriate School and family internet agreement before pupils can use IT resources. (see Appendix 3 and 4)
- Parents will be clearly informed that the use of the Internet is a statutory requirement.
- Parents will be asked to sign a permission letter to indicate that they wish their child to use the Internet.
- Parents will be asked to sign a letter to indicate that they give permission for their child's image and/or work to be used on the school website, Twitter and in school publications.
- The school will keep a record of all staff and pupils who are not granted Internet access and consent and / or permission for use of photographs and video recordings. (see Appendix 5) The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access withdrawn.

#### **Community use of the Internet**

The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

#### **E-Bullying**

The school takes bullying very seriously and has robust procedures for identifying and dealing with it. E-bullying is the use of any communication medium to offend, threaten, exclude or deride another person or their friends, family, gender, race, culture, ability, disability, identity, age or religion. Pupils are taught about bullying as part of the PSHE curriculum. We expect all members of our community to communicate with each other with respect and courtesy.

Bullying of any type will not be tolerated by the school and will be dealt with under the procedures within the Whole School Policy on Behaviour, including bullying, and also in line with the Safeguarding Policy – peer- on-peer abuse.

#### **Internet Safety:**

All parents receive a letter informing them of the school's expectations for responsible use of the internet.

When using a network workstation all access to the Internet is protected by a number of different filters. These filters are designed to prevent accidental or deliberate access to unsuitable materials. In addition, the network administrators can manually add site addresses which are considered to be unacceptable. However, no system is 100% safe and we expect users to behave responsibly.

Pupils accessing the Internet at home are subject to the controls placed upon them by their parents. However, any home use of the Internet made in connection with the school or school activities; any of its staff, pupils and governors or any partnership organisation will be subject to this policy and any breach dealt with as if the event took place at school. We expect all members of our school community to behave as positive ambassadors of the school in all school related activities made through the Internet.

The school website contains school policies, newsletters and other information. We expect all persons accessing the school web site to treat the content with respect and make no attempt to reproduce, use or alter any part in any way with malicious intent. No part can be reproduced for commercial reasons without written permission from the school.

## **Network safety**

All users need to log on using a username and password. Pupils log on using a username KS2 but have a common password. We expect all users to only log on using their username.

All staff agree to use computers in line with Rochdale's acceptable use policy as they log on. The full policy can be found on the Rochdale's schools intranet or by request from [helpdesk@edit.org.uk](mailto:helpdesk@edit.org.uk)

Each child has a folder on the 'W' drive in which they save their work to build a portfolio of evidence. Children are taught not to access other children's work without their permission.

The network software prevents changes being made to computer settings. Only the network administrators are permitted to install software on to computers.

All users of the network can be monitored remotely by the network administrators.

## **Managing Internet Access**

### **Information system security**

- School IT systems capacity and security will be reviewed annually
- Virus protection will be updated regularly
- Staff must not attempt to install new software or devices as this is the responsibility of the Edit Team.

### **Managing filtering**

- Network Connect filtering system aims to protect pupils from obscene material and information relating to the misuse of drugs and the promotion of violence, intolerance, racism and extreme political and social views.
- The school will work with the Edit Team and Network Connect to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to a senior member of staff.
- The Edit Team and Network Connect will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

### **Complaints**

Any complaints of Internet misuse will be dealt with by a senior member of staff.

If a complaint is made about staff misuse, then it shall be referred to the headteacher. Parents and pupils will need to work in partnership with staff to resolve any issues raised.

## **E-mail**

- Most classes have a Purple Mash 2email, email address which pupils can use for sending messages to other classes and other members of staff within school. The class teacher monitors the pupil's use of this email address and receives a copy of all incoming email.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- Staff will only use school email accounts for school business. Personal accounts will never be used for professional matters.
- Some pupils will have their own webmail accounts at home. As these are independent of the school they do not necessarily come with the safeguards that we set for email usage. Therefore we do not permit the use of personalised email accounts by pupils at school or at home for school purposes.

## **School Website**

The school website is an ideal tool to communicate with current parents and pupils as well as the local community and to share the achievements of all those at Shawclough Community Primary School.

- The website will be regularly checked to ensure that there is no content that compromises the safety of pupils or staff and is in line with GDPR.
- The contact details on the website will be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

- Edit and Network Connect will block/filter access to social networking sites for pupils.
- The school twitter account will be run from school devices and be led by the computing team.
- Pupils will agree through the Internet Agreement never to give out personal details of any kind which may identify them and/or their location.
- All staff agree when signing the Staff Code of Conduct to behave in a professional manner when using such sites in their personal time and are solely responsible for ensuring a high level of personal security regarding their accounts.

### **Social networking**

The school is aware and acknowledges that increasing numbers of adults and children are using social networking sites. The four with the widest use are Facebook, Twitter, Instagram and Snapchat.

The widespread availability and use of social networking application bring opportunities to understand, engage and communicate with audiences in new ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our reputation:

- That the school is not exposed to legal risks
- That the reputation of the school is not adversely affected
- That our users are able to clearly distinguish where information provided via social networking applications is legitimately representative of the school.

Social networking is targeted at older teenagers and adults.

The following are extracts from Twitter privacy policy:

*"If you are under age 13, please do not attempt to register for Twitter or provide any personal information about yourself to us. If we learn that we have collected personal information from a child under age 13, we will delete that information as quickly as possible."*

### **Social Networking applications**

- Must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.
- Must not be used in such a way as to be in breach of GDPR.
- Must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns
- Must not be used in an abusive or hateful manner
- Must not be used for actions that would put school representatives in breach of school codes of conduct or policies relating to staff.
- Must not breach the school's misconduct, equal opportunities or bullying and harassment policies
- Must not be used to discuss or advise any matters relating to school matters, staff, pupils or parents
- No staff member should have a pupil or former pupil under the age of 18 as a 'friend' to share information with
- Employees should not identify themselves as a representative of the school
- References should not be made to any staff member, pupil, parent or school activity / event unless prior permission has been obtained and agreed with the Head Teacher
- Staff should be aware that if their out-of-work activity causes potential embarrassment for the employer or detrimentally effects the employer's reputation then the employer is entitled to take disciplinary action.

## **Sexting**

'Sexting' and 'upskirting' are some of a number of 'risk-taking' behaviours associated with the use of digital devices, social media or the internet. It is accepted that young people experiment and challenge boundaries and therefore the risks associated with 'online' activity can never be completely eliminated. However, Shawclough Primary School takes a pro-active approach to help students to understand, assess, manage and avoid the risks associated with 'online activity'. The school recognises its duty of care to its young people who do find themselves involved in such activity as well as its responsibility to report such behaviours where legal or safeguarding boundaries are crossed.

There are a number of definitions of 'sexting' but for the purposes of this policy sexting is simply defined as:

- Images or videos generated by children under the age of 18,
- or of children under the age of 18 that are of a sexual nature or are indecent.
- These images are shared between young people and/or adults via a mobile phone, handheld device, computer, 'tablet' or website with people they may not even know.

The definition of 'upskirting' is "taking a picture under a person's clothing without them knowing and without their consent, with the intention of viewing their genitals or buttocks, to obtain sexual gratification or cause the victim humiliation or distress.

## STEPS TO TAKE IN THE CASE OF A SEXTING/UPSKIRTING INCIDENT

### Step 1 - Disclosure by a student

Sexting disclosures should follow the normal safeguarding practices and protocols (see Safeguarding Policy).

A student is likely to be very distressed especially if the image has been circulated widely and if they don't know who has shared it, seen it or where it has ended up. They will need pastoral support during the disclosure and after the event. They may even need immediate protection or a referral to police or social services; parents should be informed as soon as possible (police advice permitting).

The following questions will help decide upon the best course of action:

- Is the student disclosing about themselves receiving an image, sending an image or sharing an image?
- What sort of image is it? Is it potentially illegal or is it inappropriate?
- Are the school child protection and safeguarding policies and practices being followed?
- For this reason a member of the Safeguarding team should be involved as soon as possible.
- How widely has the image been shared and is the device in their possession?
- Is it a school device or a personal device
- Does the student need immediate support and/or protection?
- Are there other students and/or young people involved?
- Do they know where the image has ended up?

### Step 2- Searching a device – what are the rules?

The policy allows for a device to be examined, confiscated and securely stored if there is reason to believe it contains indecent images or extreme pornography.

#### When searching a mobile device, the following conditions should apply:

- The search is conducted by the Headteacher or a person authorised by them and one other person
- A member of the safeguarding team should always be present
- The search should normally be conducted by a member of the same gender as the person being searched. However, if the image being searched for is likely to be of a different gender to the person 'in possession' then the device should only be viewed by a member of the same gender as the person whose image it is.

If any illegal images of a young person are found the Safeguarding Team will discuss this with the Police (see Appendices 7 & 8).

The Association of Chief Police Officers (ACPO) advise that as a general rule it will almost always be proportionate to refer any incident involving 'aggravated' sharing of images to the Police, whereas purely 'experimental' conduct may proportionately dealt with without such referral, most particularly if it involves the young person sharing images of themselves.

### **Publishing pupil's images and work**

Parents and carers are required to state that they give permission for images of pupils to be electronically published. To ensure pupil's safety images that include pupils will be selected carefully and pupils' full names will not be used anywhere in the website, particularly in association with photographs. Sharing and publishing will always be in line with GDPR - see Photograph Policy.

### **Acceptable use policy for staff**

Staff need to ensure that there may be issues relating to a child's behaviour as a result of child protection issues. Where staff have any concerns of this nature the agreed steps outlined in the school's 'Child Protection Policy' should be followed.

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

**All staff to read and sign acceptable use policy. See appendices 2**

### **Acceptable use policy for pupils**

Shawclough Primary School is committed to safeguarding and promoting the welfare of children. All pupils use computer facilities including Internet access as an essential part of learning, as required by the national curriculum, therefore, gaining pupils' and parents' agreement to e-safety rules is important.

This is to be obtained once a year at the same time as checking home and emergency contact details. To ensure clarity, the e-safety Rules appropriate to the age of the pupil will be included with the letter to parents.

A list of pupils whose parents have not consented for Web publication of works and photographs and for internet access will be held in the office for staff to refer to when appropriate.

#### **Electronic Communications**

##### **Mobile Phones**

Pupils are not permitted to have mobile phones in school at any time. Pupils are aware of this fact and will be made aware of the effects and consequences of sending abusive or inappropriate text messages to others be it in or out of school time. If a mobile phone is brought onto the school premises it will be locked safely in the school safe to be collected by a parent at the end of the school day.

Staff are not permitted to use a personal mobile phone during teaching time and will ensure that they are turned off, unless in special circumstances where arrangements have been made with their line manager prior to date. No images of children will ever be taken on a member of staff's mobile phone.

### **Digital Cameras**

Staff and children regularly use digital cameras; for example to photograph events, capture pupils completing activities and to record achievements. School cameras are available for all staff and children to use. A personal camera will never be used to take photographs of pupils. Images of pupils will never be stored on any USB device but will only be saved onto the school system and accessed using the remote access scheme.

### **Managing emerging technologies**

Emerging technologies will be examined for educational benefit and a risk assessment carried out before use in school is allowed.

### **Copyright:**

Though there are lots of free to use resources on the Internet, the majority of image, sound and music files are covered by copyright laws. Some can be used for educational reasons without permission provided that the source is stated and that they are not made available outside the school. Some cannot be used under any circumstances, this is particularly so for music but can apply to other types of file e.g. photographic images. Care therefore needs to be taken with multi-media work which incorporates anything downloaded from the Internet or any other published source that it is not



uploaded onto the school's website or broadcast through any other technology. Pupils are taught that the people who put their work on the Internet may not always want people to copy or use their work and that they should check whether they have permission. We expect all users to respect copyright laws.

It is important to know what work is original and when chunks of text have been copied from other sources such as the Internet. Pupils are taught that they should not present the work of others as their own work. Older pupils are taught about copyright and how to extract or paraphrase information. We expect all pupils to make it clear what is their own work and what is quoted from other sources.

#### **Data Protection Act:**

The Data Protection Act 1998 gives you the right to access information held about you or your child by the school. Further information on the Data Protection Act can be obtained from the Department of Constitutional Affairs – [www.justice.gov.uk](http://www.justice.gov.uk).

#### **Protecting Personal Data**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and GDPR. Shawclough Community Primary School follows the guidance from Rochdale's LA including:

- using only password protected sites to pass on information
- use encrypted USB pens for anything which includes personal data e.g. report writing
- using encrypted emails for anything which includes personal data
- not using faxes to pass on any data and seeking clarification about others are using and disposing of information.

#### **Physical Safety:**

All electrical equipment in the school is tested annually to ensure that it is safe to use. Pupils are taught about the dangers of electricity as part of the science and PSHE curriculum. We expect pupils to behave appropriately near electrical sockets and appliances.

All the projectors in our school have maximum light levels below the government's health and safety guidance of 1,500 ANSI lumens. Pupils are taught that they should not look directly at strong light sources such as the sun, lasers or data projectors. We expect all users to not look directly into the light beam when working on the interactive whiteboards.

Workstations are cleaned and sanitised regularly. Pupils are taught to avoid taking food and liquids anywhere near the computers. We expect all users to refrain from eating and drinking when working at a computer.

Health and safety guidance states that it is not healthy to sit at a computer for too long without breaks. Pupils are taught correct posture for sitting at a computer and that sitting for too long at a computer can be unhealthy. We expect all users to take responsibility for their own physical well-being by adopting good practices.

Computers and other IT equipment can be easily damaged. Pupils are taught the correct way to use IT equipment. We expect pupils to respect IT equipment and take care when handling and using.

#### **Disclaimer**

The school will take all reasonable precautions to ensure that users access only appropriate material. However the school recognises that, under certain circumstances, the Internet can give staff and pupils access to undesirable information and images. We have done all that is possible to ensure children are protected from such information through the use of security software, a filtering system implemented by the Edit Team and network connect, limiting of features and construction of an Intranet, Twitter and Website that provide as safe an environment as possible. The children are taught to use the facility sensibly and with proper consideration for others through the schemes of work planned in each Unit. The school will audit IT provision to establish if the online-safety policy is adequate and that its implementation is effective.

## Disposal of equipment

Shawclough community Primary School has a software and hardware asset for both educational and administrative purposes. All equipment and software comes at a cost to the school and is therefore controlled and documented appropriately.

All IT –related assets are recorded in an inventory. Software and Hardware inventories allow the school to review what equipment and software licences we have available to us at any point in time. Hardware can be issued to staff and pupils, with serial numbers and specifications all documented as an audit trail and, where appropriate, for insurance purposes. We ensure that we are all aware of all the software licences we hold so we do not breach licensing terms and conditions as this could result in prosecution.

By maintaining inventories, we are in a position to extract full value for our purchases as educational activities can be based and planned around assets we hold. It should also not be overlooked that we record information of all equipment and this assists us in our hardware replacement programme and software upgrades, as spending and planned against assets age and specification.

All hardware such as laptops, PCs, iPads, iPods, servers and removable media needs to be formatted prior to disposal (or through a third party) to ensure no sensitive or personal data remain.

### Key steps

- Maintain an inventory of all software and hardware that the school owns. This would probably be best done in a spreadsheet.
- Consider the issues in the following statements, and discuss how you will address these within your school. Then adapt or replace the statements to reflect your approach. Any additional statements you need.

### Possible statements

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant IT equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility and destruction of any personal data.
- All redundant IT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any IT equipment will confirm to The Waste Electrical and Electronic Equipment (Amendment) regulations 2007.

Further information can be found on the Environment Agency website.

## SEND Intent

At Shawclough, we believe that every pupil, regardless of needs, disability, race or gender, has a right to equal access to a broad and balanced curriculum. We present this subject in a supportive and stimulating atmosphere, which values each child and encourages them to achieve their full potential. We recognise every child as an individual, promoting self-esteem, independence, respect and responsibility. We work closely in partnership with parents and the wider community, as we understand that this is effective in helping children to learn and develop. We encourage children to be proactive in their learning by helping them to understand what they are good at and what they can do to get better.

It is our intent for all children with additional needs to:

- Have access to a broad balanced and relevant curriculum
- Be happy and feel secure.
- Be included.
- Achieve their very best.

- Demonstrate personal development and growth.
- Make good progress based on their personalised targets and Individual Provision Map (IPM)
- Experience wider activities leading to greater independence.
- Make effective independent decisions.

## E-Safety Contacts and References

**CEOP** (Child Exploitation and Online Protection Centre): [www.ceop.police.uk](http://www.ceop.police.uk)

**Childline:** [www.childline.org.uk](http://www.childline.org.uk)

**Childnet:** [www.childnet.com](http://www.childnet.com)

**Click Clever Click Safe Campaign:** <http://clickcleverclicksafe.direct.gov.uk>

**Cybermentors:** [www.cybermentors.org.uk](http://www.cybermentors.org.uk)

**Digizen:** [www.digizen.org.uk](http://www.digizen.org.uk)

**EiS** - ICT Support for Schools and ICT Security Advice: [www.eiskent.co.uk](http://www.eiskent.co.uk)

**Internet Watch Foundation** (IWF): [www.iwf.org.uk](http://www.iwf.org.uk)

**Kidsmart:** [www.kidsmart.org.uk](http://www.kidsmart.org.uk)

**Teach Today:** <http://en.teachtoday.eu>

**Think U Know website:** [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)

**Virtual Global Taskforce** — Report Abuse: [www.virtualglobaltaskforce.com](http://www.virtualglobaltaskforce.com)

Appendices

Appendix 1 : Think Then Click Rules

# Key Stage 1

These rules help us to stay safe on the Internet

## Think then Click



We only use the Internet when an adult is with us.



We can click on the buttons or links when we know what they do.



We can search the Internet with an adult.



We always ask if we get lost on the Internet.



We can send and open emails together.



We can write polite and friendly emails to people that we know.



B. Stoneham & J. Barrett

# Key Stage 2

## Think then Click



We ask permission before we use the internet.

We only use websites that our teacher has chosen.



We immediately close any websites we don't like.

We only e-mail people our teacher has approved.



We will send messages that are polite and friendly.

We never give out home address or phone number.



We never arrange to meet anyone we don't know.

We never open messages sent by anyone we don't know.



We never use Internet chat rooms.

We will tell the teacher if we see anything we are unhappy with.



Appendix 2

Appendix 3

SHAWCLOUGH COMMUNITY PRIMARY SCHOOL

SCHOOL AND FAMILY INTERNET AGREEMENT

CHILD'S NAME: \_\_\_\_\_

DATE OF BIRTH: \_\_\_\_\_

I agree to follow these rules and my parent/carer/teacher agrees to help me follow these rules when I use the Internet or mobile phone:

\* I agree to keep all personal information private – including my name, home address, school address, e-mail, home and mobile phone numbers and passwords.

\* I agree not to visit sites that I know I shouldn't and log out straight away if I come across such a site accidentally. I will then tell my parent/carer.

\* I agree not to download unknown files from the Internet without getting permission from my parent/carer.

\* I agree not to send any photographs of myself, my friends or any other members of the family to anyone on the Internet or by mobile phone without asking permission from them first.

\* I agree not to take pictures or videos with my mobile phone of my friends without asking their permission.

\* I agree not to download files that I know I shouldn't (such as copyright music/games/films).

\* I agree to ask my parent/carer before registering or signing up for things online including competitions.

\* I agree to tell my parent/carer if I receive frightening or bullying text messages or emails or any message that upsets me, makes me feel awkward, uncomfortable or pressurises me (regardless of what I might have said to this person already).

\* I agree to respect other people that I am talking to online and I won't send nasty messages to other people.

\* I agree to only have buddies on my instant messenger that I know in the real world and remember that an online friend is a stranger in the real world, so I will never arrange to meet someone I have met via the Internet without my parent/carer's knowledge and permission.

\* I agree to stop using the Internet when my parent/carer tells me to and to share it with other members of my family.

\* I agree only to visit websites that my parent/carer has agreed to.

I promise to help my child follow these rules.

\_\_\_\_\_

(Signed by parent/carer)

## Appendix 4

SHAWCLOUGH COMMUNITY PRIMARY SCHOOL

SCHOOL AND FAMILY INTERNET AGREEMENT

CHILD'S NAME: \_\_\_\_\_

DATE OF BIRTH: \_\_\_\_\_

I agree to follow these rules and my parent/carer/teacher agrees to help me follow these rules when I use the Internet or mobile phone:

- \* I agree to keep all personal information private – including my name, home address, school address, e-mail, home and mobile phone numbers and passwords.
- \* I agree not to visit sites that I know I shouldn't and log out straight away if I come across such a site accidentally. I will then tell my parent/carer.
- \* I agree not to download unknown files from the Internet without getting permission from my parent/carer.
- \* I agree not to send any photographs of myself, my friends or any other members of the family to anyone on the Internet or by mobile phone without asking permission from them first.
- \* I agree not to take pictures or videos with my mobile phone of my friends without asking their permission.
- \* I agree not to download files that I know I shouldn't (such as copyright music/games/films).
- \* I agree to ask my parent/carer before registering or signing up for things online including competitions.
- \* I agree to tell my parent/carer if I receive frightening or bullying text messages or emails or any message that upsets me, makes me feel awkward, uncomfortable or pressurises me (regardless of what I might have said to this person already).
- \* I agree to respect other people that I am talking to online and I won't send nasty messages to other people.
- \* I agree to only have buddies on my instant messenger that I know in the real world and remember that an online friend is a stranger in the real world, so I will never arrange to meet someone I have met via the Internet without my parent/carer's knowledge and permission.
- \* I agree to stop using the Internet when my parent/carer tells me to and to share it with other members of my family.
- \* I agree only to visit websites that my parent/carer has agreed to.

I promise to follow these rules. I promise to help my child follow these rules.

---

(Signed by child)

(Signed by parent/carer)

## Appendix 5

### SHAWCLOUGH COMMUNITY PRIMARY SCHOOL

#### POLICY AND GUIDANCE ON PHOTOGRAPHS OF CHILDREN

Manager: Julia Sandiford-Mitchell

Reviewed April 2020  
 Approved by Governors  
 Next review April 2023

#### INTRODUCTION AND LEGAL FRAMEWORK

The Headteacher acknowledges and thanks Warwickshire County Council for its support and help on the production of this policy.

This policy has been written in accordance with NSPCC guidelines.

Under the legal obligations of the General Data Protection Regulation (GDPR), the school has specific responsibilities in terms of how photos and videos are taken, stored and retained.

The aim of this document is to provide guidance on the appropriate use of images of children in School. This policy is applicable to all forms of visual media, including film, print, video, DVD and websites and social media sites wherever they are used. The guidance is for all Shawclough staff (including, the governing body, teachers, support staff, external contractors, visitors and volunteers) as well as children and parents/carers who wish to use images of children and young people in education.

We need to make proper use of photographic images while meeting the law and preserving the safety of children. Concerns focus on issues around rights of:

- a. privacy, including data protection
- b. child protection and safeguarding
- c. copyright ownership

These guidelines address these issues.

#### TYPICAL USES OF PHOTOGRAPHS

At Shawclough we use photographs and video recordings for a range of purposes some of which might include:

- Developing key skills in different curriculum and pastoral areas.
- To develop portfolios and learning journeys in children's books or teacher files, including providing evidence for statutory teacher assessments.
- Recording concerts, celebration events, sports days and sports fixtures
- Providing the media, including newspapers and television with images from events or projects.
- Displays in the School of children's activities.
- Publications by the School.
- School's website.
- Staff training and professional development activities.
- School approved websites for sharing information and achievements e.g. Twitter.

Events are also photographed by parents and carers and children from both Shawclough and other schools usually to add to their own collections.

#### ROLES AND RESPONSIBILITIES

The Data Protection Officer (DPO) Sara Conway, supported by the Senior Leadership team, is responsible for ensuring the acceptable, safe use and storage of photographs and videos including

- Informing, advising and training staff about their obligations to comply with GDPR.
- Monitoring the school's compliance with the GDPR.

The Designated Safeguarding Lead (DSL) Julia Sandiford-Mitchell is responsible for

- Liaising with social workers to gain consent for photography and videos of LAC pupils.
- Informing relevant staff of any known changes to a pupil's security, e.g. child protection concerns, which would mean that participating in photography and video recordings would put them at significant risk.

All staff are responsible for being aware of children who do not have parental permission for photographs and videos and those children should not be included in photographs or videos

#### PARENTAL PERMISSION

1. Use of images of children require the consent of the parent / carer.
2. Shawclough obtains permission from all parents and carers of children when their child first enters the School. They are given the "Parental consent for photographs and video recordings to be taken of their child" form to complete and return to the school. These consents are maintained in the School Office.
3. Each year as part of a School Newsletter the School will inform parents of the opportunity to change their permission. Any parents who do will be encouraged to contact the Headteacher.

4. When a parent does not agree to their child being photographed, the Headteacher will inform staff and make every effort to sensitively comply with the request.
5. When photographic images are transmitted or shared beyond the establishment e.g. television broadcasts, specific permission will be obtained from parent.

#### GUIDANCE TO STAFF TAKING PHOTOGRAPHS OR VIDEO RECORDINGS

1. Before taking a picture the Member of staff must where appropriate, obtain the consent of the person in the picture.
2. When photographing children:
  - a. Ensure that parents and carers of the children have signed and returned the consent form for general photography.
  - b. Ensure all children are appropriately dressed.
  - c. Avoid images that only show a single child with no surrounding context of what they are learning or doing.
  - d. Photographs of three or four children are more likely to also include their learning context.
  - e. When using photographs as evidence for teacher assessments consider taking the photograph from behind the child – so the learning in the activity is the focus not the child themselves.
  - f. Do not use images of a child who is considered very vulnerable unless parents / carers have given specific written permission.
  - g. Avoid naming young people. If one name is required, then use the first name only where possible.
  - h. Use photographs that represent the diversity of the young people participating.
  - i. Report any concerns relating to any inappropriate or intrusive photography to the head teacher / manager.
  - j. Remember the duty of care and challenge any inappropriate behaviour or language.
  - k. Do not use images that are likely to cause distress, upset or embarrassment.
  - l. Remember to store images on password protected, school devices.
  - m. Use the image in its intended context. (An example of this not happening is when a picture taken by a national newspaper of a child accepting an award was used by the National Front for a completely different story.
  - n. Regularly review stored images and delete unwanted material.
  - o. Follow the commitment made in the consent forms:
    - a) not to name the child.
    - b) not to use the photograph out of context.
    - c) not to use the photograph to illustrate sensitive or negative issues.

#### INTER-SCHOOL EVENTS

Apply these guidelines to inter-school events. If a vulnerable child is involved, it will be necessary to liaise with a member of staff from the other establishment so that they are aware of the wishes of the parents or carer of the child and seek the cooperation of the parents of the opposing team.

#### TEACHER TRAINING AND PORTFOLIOS

During teacher training and with newly qualified staff, colleagues may need to compile portfolios with photographs of children during lessons. Staff should act responsibly and in accordance with these guidelines in compiling these images. The member of staff mentoring the colleague will oversee the compiled images as part of the management process and consider their appropriateness.

#### DISPLAYS IN SCHOOLS

Still photographs shown on displays and video clips available during open / parents' evenings should depict children in an appropriate way. They should not display images of children in inappropriate or revealing clothing so appropriate levels of integrity and decency are maintained. Do not use photographs or images likely to cause embarrassment.

#### PARENTS EVENINGS, CONCERTS, PRESENTATIONS

Parents will be permitted to take photographs of children during such events. However, it will be necessary to ensure:



- that the children in the event and being photographed have sent into school a completed obtain parental permission form.
- ensure that children are appropriately dressed.
- be aware of any child who should not be photographed and ensure that they are not being photographed.
- monitor the use of cameras and anyone behaving inappropriately.
- Visitors/parents are told NOT to put images of other people's children on social media and the internet, in any way.

#### CHILDREN PHOTOGRAPHING EACH OTHER

This practice can occur during offsite activities. Staff should maintain the supervision, manage and control the situation with care. There may be incidents where children take inappropriate photographs, perhaps showing friends and other children inappropriately dressed. Staff should endeavour to discourage this practice, but ultimately parents are responsible for monitoring their child's use of their own cameras and phones and subsequent use of their images involved.

#### NEWSPAPERS AND OTHER PUBLICATIONS

Several scenarios can occur:

##### 1. Team photographs:

- When everyone is prepared to allow team photographs and full names to be published. In this situation publication can occur.
- If a parent is not happy to have a child's name printed on a photograph, then consideration could be given to publishing the photograph with no names. The head teacher / manager should make every effort to ensure, in conjunction with the newspaper editors, that this occurs.
- If parents of a child have indicated that the child is vulnerable and should not have a photograph printed, then a team photograph may not be appropriate.

##### 2. Photo opportunities:

- When an establishment invites a newspaper to celebrate an event, the head teacher / manager should make every effort IN ADVANCE to ensure that the newspaper's requirements can be met.
- Almost without exception, this means the paper will prefer to publish the full names of anyone in a photograph they print. The only exception to this might be (as above) in a larger group shot (e.g.: a group of more than 10 children).
- However, newspapers usually prefer to work with smaller groups of children – e.g.: three or four – and for this number names would definitely be required.
- It is not acceptable to invite a newspaper to take photographs and then refuse to provide any names. Newspapers will not print anonymous photographs. Establishments must give thought to this beforehand – and parental permission / opinion must be their key guidance.
- This might mean offering only those children whose parents are happy for publication of photographs and names for inclusion in any photo opportunities.
- If this is not possible – for instance because a specific group of children have achieved something, and parental permission re. the publication of full names is withheld for one or more of the group - it might be possible to negotiate a 'first names only' agreement with the newspaper.
- Otherwise establishments must be prepared to forego newspaper publicity.

#### MOBILE PHONES

The children are not permitted to use mobile phones in school and therefore the possibility of using phones with photographic capabilities is restricted.

However parents or other who may have such equipment will be reminded that the use of mobile phones which contain cameras will not be permitted in changing rooms, toilets etc.

Staff are only to use school equipment e.g. cameras and ipads, to photograph/film children. If, for any reason, personal devices are used, the images must be deleted before leaving the school premises and NEVER stored on personal equipment, e.g. laptops.

## Appendix 6

### The Legal Position

It is important to be aware that young people involved in sharing sexual videos and pictures may be committing a criminal offence. Specifically, crimes involving indecent photographs (including pseudo images) of a person under 18 years of age fall under Section 1 of the Protection of Children Act 1978 and Section 160 Criminal Justice Act 1988. Under this legislation it is a crime to:

- take an indecent photograph or allow an indecent photograph to be taken;
- make an indecent photograph (this includes downloading or opening an image that has been sent via email);
- distribute or show such an image;
- possess with the intention of distributing images;
- advertise; and
- possess such images

While any decision to charge individuals for such offences is a matter for the Crown Prosecution Service, it is unlikely to be considered in the public interest to prosecute children. However, children need to be aware that they may be breaking the law. Although unlikely to be prosecuted, children and young people who send or possess images may be visited by police and on some occasions media equipment could be removed. This is more likely if they have distributed images.

The decision to criminalise children and young people for sending these kinds of images is a little unclear and may depend on local strategies. However, the current Association of Chief Police Officers (ACPO) position is that: 'ACPO does not support the prosecution or criminalisation of children for taking indecent images of themselves and sharing them. Being prosecuted through the criminal justice system is likely to be upsetting and distressing for children especially if they are convicted and punished. The label of sex offender that would be applied to a child or young person convicted of such offences is regrettable, unjust and clearly detrimental to their future health and wellbeing.'

## Appendix 7

Shawclough Primary School

SEXTING POLICY

February 2016

Shawclough Primary School Sexting Policy Page 10

However, there are cases in which children and young people have been convicted and sent to prison. The important thing to remember is that whilst, as a school, we will want to consider the implications of reporting an incident over to the police, it is not our responsibility to make decisions about the seriousness of the matter; that responsibility lies with the Police and the CPS hence the requirement for the school to refer.

In summary sexting is classed as illegal as it constitutes sharing and/or possessing an indecent image of a child

## Appendix 8

### Data Protection Privacy Notices

Organisations that use pupil data have to comply with the GDPR. This means that the data held about pupils must only be used for specific purposes allowed by law. We are therefore telling you about the types of data held, why that data is held, and to whom it may be passed on.

A number of organisations require access to data in the Learner Registration Scheme in order to run their education system and process information on pupils.

These include:

- Schools
- Local Authorities (LAs)
- Department for Education (DfE)

- Ofsted
- Young People's Learning Agency (YPLA)

The Department of Health (DoH) and Primary Care Trusts (PCTs) process information on pupils in order to tackle the year on year rise in obesity among children.

The school holds information on pupils in order to support their teaching and learning, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well the school as a whole is doing. This information includes:

- Contact details
- National curriculum assessment results
- Public examination results
- Attendance information
- Characteristics (such as ethnic group)
- Special educational needs
- Any relevant medical information

From time to time schools are required to pass on some of this data to Local Authorities, the Department for Education and to agencies that are prescribed by law, such as Ofsted, Young People's Learning Agency, Department of Health and Primary Care Trusts.

#### Local Authority

The Local Authority uses information about children for whom it provides services to carry out specific functions for which it is responsible, such as the assessment of any special educational needs the child may have. It also uses the information to derive statistics to inform decisions on (for example) the funding of schools, and to support teaching and learning. The statistics are used in such a way that individual children cannot be identified from them. The LA have a duty under the Childrens Act 2004 to co-operate with their partners in health and youth justice to improve the well being of children in their areas.

#### Contact

Information Governance Unit  
[foi@rochdale.gov.uk](mailto:foi@rochdale.gov.uk)

#### Department for Education (DfE)

The Department for Education uses information about pupils for research and statistical purposes, to inform, influence and improve education policy and to monitor the performance of the education service as a whole. This includes the Key Stage assessments for pupils in primary and secondary schools. They will feed back to LAs and schools, information about their pupils for a variety of purposes that will include data checking exercises, use in self-evaluation analyses and where information is missing because it was not passed on by a former school.

The DfE will also provide Ofsted with pupil data for use in school inspection. Where relevant, pupil information may also be shared with post 16 learning institutions to minimise the administrative burden on application for a course and to aid the preparation of learning plans.

Pupil information may be matched with other data sources that the Department holds in order to model and monitor pupils' educational progression; and to provide comprehensive information back to LAs and learning institutions to support their day to day business. The DfE may also use contact details from these sources to obtain samples for statistical surveys: these surveys may be carried out by research agencies working under contract to the Department and participation in such surveys is usually voluntary. The Department may also match data from these sources to data obtained from statistical surveys.

Pupil data may also be shared with other government departments and agencies (including the Office for National Statistics) for statistical or research purposes only. In all these cases the matching will require that individualised data is used in the processing operation, but that data will not be processed in such a way that it supports measures or decisions relating to particular individuals or identifies individuals in any results. This data sharing will be approved and controlled by the DfE Chief Statistician.

The DfE may also disclose individual pupil information to independent researchers into the educational achievements of pupils who have a legitimate need for it for their research, but each case will be determined on its merits and subject to the approval of the Department's Chief Statistician.

## Contact

### Data and Statistics Division (DSD) Helpdesk

1st Floor Mowden Hall, Staindrop Road, Darlington DL3 9BG

Tel: 01325 392626

[dsd.helpdesk@education.gsi.gov.uk](mailto:dsd.helpdesk@education.gsi.gov.uk)

### Department for Education

Pupils under 12 years old as data subjects have rights under the GDPR, including a general right of access to personal data held on them, with parents exercising this right on their behalf if they are too young to do so themselves. If you wish to access the personal data held about your child, please contact the relevant organisation in writing.

Pupils over 12 years old as data subjects, have certain rights under the GDPR including a general right of access to personal data held on them. If you wish to access your personal data, or you wish your parents to do so on your behalf, then please contact the relevant organisation in writing.