Tividale Community Primary School

Online Safety Policy

Purpose of our Online Safety Policy

Rationale

As the use of online services and resources grows, so has awareness of the risks and potential dangers which arise from the use of communications technology and the internet. Those risks are not confined to the use of computers; they may also arise through the use of other handheld devices such as games consoles, mobile phones and tablets.

Children and adults interact with new technologies on a daily basis. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial but can occasionally, if not used correctly, place children, adults working with children and parents at risk.

Our Online Safety Policy covers issues relating to safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes educating all on the risks and responsibilities of using such technologies safely and is part of the "duty of care" which applies to everyone working with children. Tividale Community Primary School will also provide safeguards and rules to guide staff, pupils, parents and visitors in their online experiences. This policy also gives guidelines and expectations in the use of social media.

Online Safety at Tividale Community Primary School is embedded in effective practice in each of the following areas:

- Education for responsible ICT use by all staff and pupils;
- A comprehensive, agreed and implemented policy;
- Use of a secure, filtered broadband;
- A school network that complies with the National Education Network standards and specifications;
- Safeguarding.

The policy is one of the strategies Tividale Community Primary has in place to promote the safeguarding of learners in their care both when they are in the school and when they are elsewhere.

Communications of this Policy

This Online Safety Policy has been written by the school, building on Local Authority and government guidance and through period of consultation with staff. It will be approved by Governors and the School Leadership Team. This policy will be available on the school's website and on Office 365, and has been read by all staff.

Parents will be made aware that the school has an Online Safety policy and will be advised on ways of keeping their children safe at home.

It is the responsibility of all staff and pupils to ensure that they use communications technology and the internet safely and responsibly. To this end, all staff and pupils agree to an acceptable use policy (AUP).

Introducing the Online Safety Policy to pupils:

- Online Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- Online Safety will be taught based on the materials from the Child Exploitation and Online Protection Centre (CEOP.)
- Online Safety training will be embedded within the whole school curriculum.
- All children and young people require safe opportunities to understand the risks and benefits of the Internet and to balance these in their everyday use.

Staff and the Online Safety policy:

- All staff will be given the School's Online Safety policy and emphasise its importance.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Where appropriate, staff will always try use a child friendly, safe search engine when accessing the web with pupils.
- Regular Online Safety training will be part of the school's Continuing Professional Development (CPD) programme.

Parents and the Online Safety Policy:

- Parents' and carers' attention will be drawn to the school's e-Safety policy in newsletters and on the school's web site.
- The school will via the school website, signpost parents to useful links.
- Online Safety support, guidance, advice and/or workshops will be offered to parents/carers with an Online Safety support contact available on the school's website.

Tividale Community Primary School's Online Safety Policy	
Revised by:	**Emma Burnell**
It was approved by the Governors on:	March 2017
The next review date is (at least annually):	March 2018
Disseminated to all staff on:	March 2017

Signed:	Date:	22/3/17	(Head Teacher)
Signed:	Date:	22/3/17	(Chair of Governors)

1. Internet Use in School

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 use of the internet and digital communications is a part of the statutory curriculum and a necessary tool for staff and pupils.

The purpose of Internet use at Tividale Community Primary School is to:

- Raise educational standards
- Promote achievements
- Support the professional work of staff
- Enhance management systems
- Provide information to parents and the wider community

Children also use the Internet regularly outside school to support their learning as well as for recreational reasons. The quality of the information received via the internet is variable. It is really important, therefore, for children to be taught the appropriate skills to select and evaluate internet content. It is also important that children know that they should report any unsuitable material to an adult immediately.

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Online Safety **Actions**

In the curriculum at Tividale Community Primary School, pupils will:

- Be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- Be educated in the effective use of the Internet to research, including the skills of retrieval and evaluation.
- Be shown how to publish and present information to a wider audience.
- Be taught how to evaluate the relevance, accuracy and quality of Internet sourced material
- Be taught the importance of cross-checking information before accepting its accuracy
- Be supervised when using the Internet
- Be taught how to report unpleasant Internet content by using the Child Exploitation and Online Protection Centre (CEOP) “Report Abuse” icon or similar systems.
- Know what to do if they experience any issues whilst online
- Sign and agree an Acceptable Use Policy (AUP)

***The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use*.**

2. Managing Internet Access

a. Information system security:

It is important that a school reviews and maintains the security of the whole computer and ICT system. This ensures the on-going delivery of essential learning services as well as the personal safety of staff and pupils. Maintaining computer security is a major responsibility of a school. It is a complex matter and will not be covered in full in this document.

Online Safety Actions

- The security of the school's information systems is reviewed regularly by the Computing Technician, Computing Leader, Head Teacher
- Virus protection is updated regularly
- Use of the Learning Platform on Office 365 ensures that all data stored on the platform is secure.
- Files held on the school's network are regularly checked and modified or deleted when necessary
- Managing filtering:

    - The school will work with Sandwell Inspired Partnerships – SIPS IT and a managed filtering system (Trustnet) to ensure systems in place to protect pupils are reviewed and improved.
    - If staff or pupils come across unsuitable on-line materials, the site must be reported to the Online Safety Co-ordinator or the Head Teacher.
    - Children are taught to turn off the monitor immediately when any unsuitable material appears, and then notify an appropriate adult.
    - Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
    - Head Teacher controls website access and requests for un restricting websites must be made on the appropriate form.

b. E-mail:

E-mail is an essential means of communication for both staff and pupils however the implications of e-mail use in school need to be thought through and appropriate measures put in place. E-mails can be difficult to monitor but unregulated e-mail can leave pupils exposed to influences outside what is acceptable in school.

Online Safety Actions

- Children only use their Learning Platform Office 365 e-mail accounts
- Pupils will be given a username and password to use the email facility on Office 365, the schools Learning Platform
- Children tell an adult immediately if they receive an offensive e-mail
- Children do not reveal personal details about themselves or others in e-mails or arrange to meet with a specific person
- Incoming e-mails to children should be treated as suspicious and attachments not opened unless the author is known
- The forwarding of chain letters is not permitted
- All staff emailing pupils copy the email to the Computing co-ordinator for monitoring purposes

c. Published content and the school web site:

Tividale Community Primary will regularly publish information, resources and national tests results on the school's management system, website and Learning Platform Office365.

Personal information should only be held on secure systems which are accessed by authorised staff whereas general information about the school may be published wider. Office365 is an effective way of publishing information relevant to the school, families and community as it requires authentication while reaching a wide and relevant audience however, sometimes it is useful to use the website. In these cases consideration of personal and school security is essential.

OnlineSafety Actions

- The contact details on the website https://tividale-pri.sandwell.sch.uk and the office e-mail and telephone number. Staff or children's personal information is not shared.
- The Head Teacher has overall editorial responsibility for the website to ensure that content is accurate and appropriate
- Parents or carers give written permission for images of children and their work to be posted on the website, pupil and family portals unless individual pupils cannot be clearly identified

d. Social networking and personal publishing:

Parents and teachers need to be aware that the Internet has online spaces and social networking sites which allow children to publish content (eg, photos, comments and personal information). These sites should only be viewed by invited 'friends'. All staff should amend settings to ensure their status and photos cannot be shared by anyone, by using networking sites and permissions settings.

When used by responsible adults social networking sites provide easy to use free facilities however children should be encouraged to think about the issues related to uploading personal information before signing up to social networking. Children are discouraged to sign up to online spaces or social networking sites.

OnlineSafety Actions

- The school blocks access to general social networking sites
- Children are taught about the dangers (including bullying) of sharing personal information, especially on-line
- Staff who use social networking sites must be aware of the nature of what they are publishing on-line in relation to their professional position
- If staff are signed up to social networking sites they must not discuss any matters relating to the school, children or their professional role on-line.
- Staff do not invite children to be 'friends' on-line and equally do not accept requests for friendship from children or former pupils of the school.
- Where necessary, the school will closely control access to and the use of school accepted social networking sites, with consideration given as to how the pupils can be educated in their safe usage.
- Pupils and staff will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils will be taught not to meet anyone first met online without specific permission or a responsible adult present.
- Pupils are encouraged to only ever use moderated social networking sites.
- Pupils and parents will be strongly advised of age restrictions of social networking sites that the use of social network spaces outside school may bring a range of dangers to all pupils.
- Webcam use will be appropriately supervised for the pupils' age and will be in line with curriculum requirements.

e. Managing emerging technologies:

Many emerging communications technologies offer the potential to develop new teaching and learning tool, including mobile communications and multimedia. A risk assessment needs to be undertaken by the IT Technician and Computing Co-ordinator, on each new technology before using it with

children. The safest approach is to deny access until a risk assessment has been completed and safety demonstrated.

Online Safety Actions

- Emerging technologies are examined for educational benefit and a risk assessment will be carried out before use in school is permitted
- If mobile phones are brought into school by children for safety purposes getting to and from school, they are placed in the school safe then returned at the end of the school day
- Personal mobiles and personal digital cameras should not be used to record sound and images during the school day
- The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new access route to undesirable material and communications.
- When mobile technology is used in the classroom, clear ground rules must be established for its safe and appropriate use.
- School digital cameras are not to be taken off the school site (with the exception of school trips).
- Any photographs or videos taken on any handheld devices are to be used in school for educational purposes only, or to create a record of children's activities for use in class or to be uploaded onto the website. Once photographs or videos are downloaded from a handheld device, they will be deleted from that device. In particular, any handheld devices which are taken off school premises, must be cleared of school photos before being removed.
- The appropriate use of Learning Platforms will be reviewed as the technology becomes available within the school.
- Pupils will be given a username and password to access Office365, the school's Learning Platform.
- The educational benefits of mobile technology will be encouraged but not misused.

f. Families and Community Use

The school values the need for Internet access to be made available at home for the children. In addition access may be available through the school library, the local library, youth services, adult education centres and supermarkets**.**

Online Safety Actions

- The school will liaise with the local authority and local organisations such as the police, to establish a common approach to e-safety in conjunction with the online safety pledge
- Parents' and carers' attention will be drawn to the school's e-Safety policy in newsletters, the school brochure and on the school's web site.

- e-Safety support, guidance, advice and/or workshops will be offered to parents/carers with an e-Safety support contact available on the school's website.

3. Leadership in online safety

a. Data Protection:

The quality and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is handled properly. The Head Teacher is responsible for ensuring the Data Protection procedures are in place.

Online Safety Actions

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998
- Staff will not store data related to children, families or school on a removable storage device.

b. Complaints Procedure

Keeping in line with school policy, if a member of staff, child, parent or carer has a complaint relating to online safety then it will be considered and prompt action will be taken following an immediate investigation.

Online Safety Actions

- Parents will be provided with advice through online-safety meetings or workshops
- Parents will be made aware of the schools online safety policy and the AUP agreements signed by children
- The school liaises with local schools and organisations to establish a common approach to online safety.
- The school will offer parents and families advice on matters of online safety e.g, social networking sites and monitoring child access at home.
- Parents will work in partnership with school and will be asked to sign a Parent AUP when their child joins school and on an annual basis thereafter.
- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. (Appendix 1 displays a flowchart of responses to an incident of concern.)

- Pupils and parents will be informed of consequences for pupils misusing the Internet.

c. Authorising Internet access:

Online safety Actions

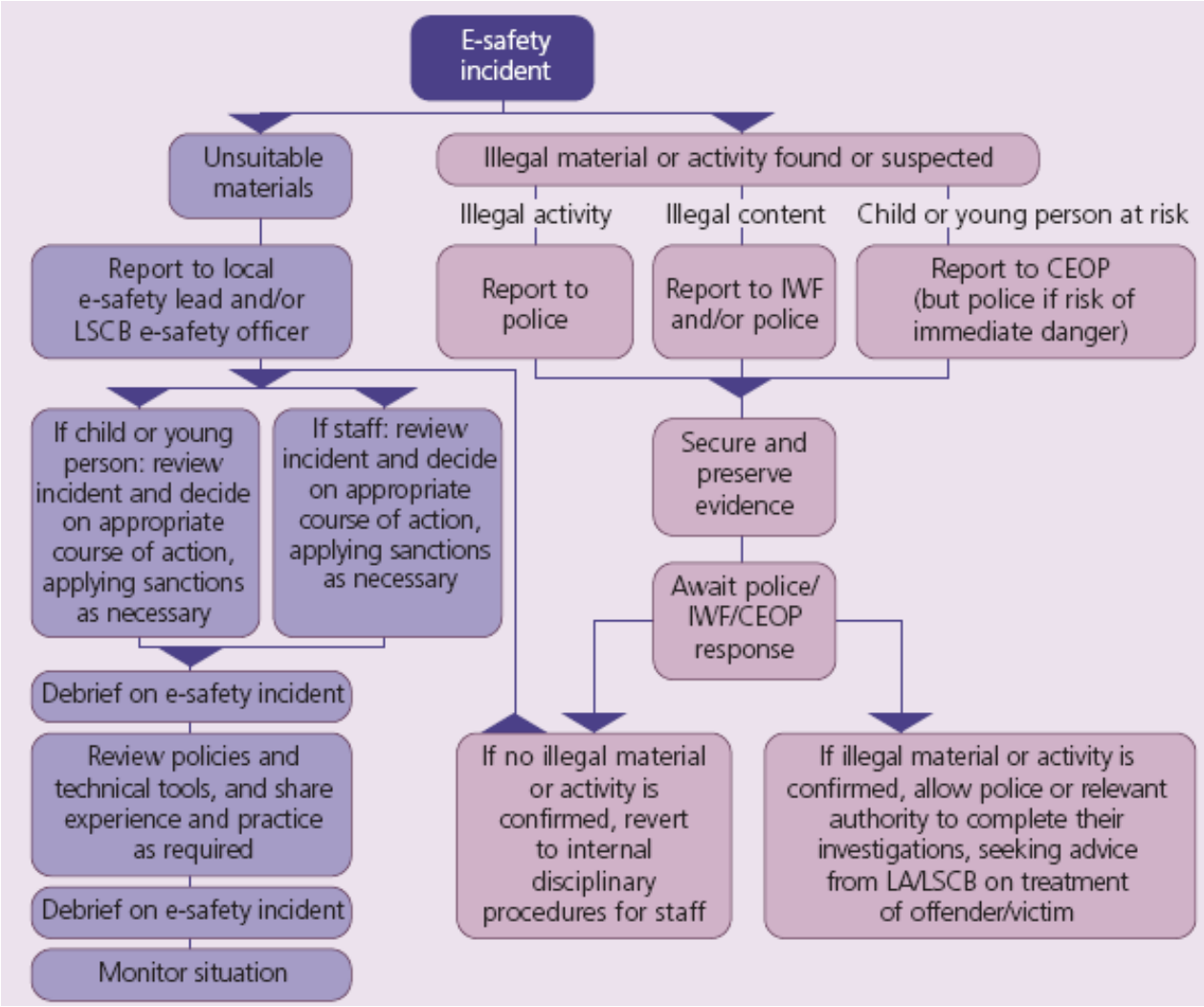
- All staff must read and sign the Staff Acceptable Use Policy for IT before using any school IT resource.
- All pupils aged 7 -11 years must sign the school AUP before being granted Internet access.
- At Tividale Community Primary School, access to the Internet will be with adult supervision and will only access specific, approved on-line materials.

d. Assessing risks:

Online safety Actions

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor Sandwell Local Authority can accept liability for any material accessed or any consequences of Internet access.
- The school will carry out an annual audit of IT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate and effective.

Appendix 1: Flowchart for responding to online safety incidents



(Figure reproduced from Becta - *Safeguarding children online: a guide for Local Authorities and Local Safeguarding Children Boards*, page 27, appendix B)

Appendix 2: Online Safety Audit

Has the school an online safety Policy in conjunction with Sandwell Local Authority?	**Y**
The school online safety policy was agreed on:	22/3/17
The policy is available for staff on:	Office 365
The policy is available for parents/carers:	Website
The responsible member of the Senior Leadership Team is:	E Burnell
The responsible member of the Governing Body is:	J Brown
The Designated Safeguarding Lead is:	E Burnell
The online safety lead in school is:	E Burnell
Has online safety training been provided for pupils?	**Y**
Has online safety training been provided for staff?	**Y**
Is there a clear procedure for a response to an incident of concern?	**Y**
Have online safety materials been obtained from recommended providers?	**Y**
Do all staff sign an Acceptable Use Policy on appointment?	**Y**
Are all pupils aware of the School's online safety rules and acceptable use policy?	**Y**
Are online safety rules or Acceptable Use Policies displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	**Y**
Do parents/carers sign and return an agreement that their child will comply with the School online safety rules and acceptable use policy?	**Y**
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	**Y**
Has an IT security audit been initiated by the Senior Leadership Team, possibly using external expertise?	**Y**
Is personal data collected, stored and used according to the principles of the Data Protection Act?	**Y**
Is Internet access provided by an approved educational Internet service provider which complies with Department for Education (DfE) requirements.	**Y**
Has the school-level filtering been designed to reflect educational objectives and approved by the Senior Leadership Team?	**Y**
Is anti-virus up-to-date, and installed on all devices?	**Y**
Are all shareholders aware of the CEOP Report Abuse button?	**Y**

Appendix 3: Useful resources for teachers

Child Exploitation and Online Protection Centre
www.ceop.gov.uk

Childnet
www.childnet-int.org

Think U Know
www.thinkuknow.co.uk

Internet Safety Zone
www.internetsafetyzone.com

Appendix 4: Acceptable Use Policies

Acceptable Use Policy
(Communications Technology and the Internet)

Adults working with young people

I agree that I will:

- Always log off a computer when leaving, even if it is only for a short while
- Only use personal data securely
- Educate children in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Educate children in the recognition of bias, unreliability and validity of sources
- Actively educate learners to respect copyright law
- Only use approved school OPENHIVE e-mail accounts in school and for school related emails
- Only use pupil images or work when approved by parents and in away that will not enable individual children to be identified
- Only give access to appropriate users when working with blogs or wikis etc
- Report unsuitable content or activities to the computing coordinator/computing technician
- Pass on any examples of Internet misuse to a senior member of staff
- Ensure that any personal use of ICT does not interfere with my professional duties or use physical resources

I agree that I will not:

- Share my password with others or work on a computer using someone else's password, unless they are overseeing the work
- Store data relating to the children, families or school on a removable storage device (eg data stick)
- Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- pornography (including child pornography)
- promoting discrimination of any kind
- promoting racial or religious hatred
- promoting illegal acts
- breaching any Local Authority/School policies, eg, gambling
- doing anything which exposes children to danger
- any other information which may be offensive to colleagues

- forward chain letters
- breach copyright law
- knowingly distribute a computer virus
- install hardware or software without permission from the Computing Coordinator, Computing technician or Head Teacher

I accept that my use of the school and Local Authority ICT facilities will be monitored and the outcomes of the monitoring may be used. I also accept that whatever I save to the Network maybe modified or deleted without my consent.

Signed: *Date:*

Acceptable Use Policy
(Communications Technology and the Internet)

School Leaders and Governors

School Leaders including Governors will ensure that:

- learners are encouraged to enjoy the safe use of digital technology to enrich their learning
- learners are made aware of risks and process for safe digital use
- the school has appointed an e-Safety team and a named governor takes responsibility for e-Safety
- an e-safety Policy has been written by the school
- the e-Safety Policy and its implementation will be reviewed annually
- the school internet access is designed for educational use and will include appropriate filtering and monitoring
- copyright law is not breached
- learners are taught to evaluate digital materials appropriately
- parents are aware of e-safety
- parents will be informed that all technology usage may be subject to monitoring, including URL's and text
- the school will take all reasonable precautions to ensure that users access only appropriate material
- the school will audit use of technology to establish if the e-safety policy is adequate and appropriately implemented
- methods to identify, assess and minimise risks will be reviewed annually
- complaints of internet misuse will be dealt with by senior member of staff

Signed: *Date:*

Acceptable Use Policy
(Communications Technology and the Internet)

Pupils (age 7-11)

I agree that I will:

- always keep my password a secret
- only visit sites which are appropriate to my learning
- work in collaboration only with friends and I will deny access to others
- turn the monitor off and tell a responsible adult straight away if anything makes me feel scared or uncomfortable online
- make sure all messages I send are respectful
- show a responsible adult if I get a nasty message or get sent anything that makes me feel uncomfortable
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my/or my parents mobile phone number to anyone who is not a friend
- only e-mail people I know or those approved by a reasonable adult
- only use an e-mail account which has been provided by school
- talk to a responsible adult before joining chat rooms or networking sites
- always keep my personal details private (my name, family information, journey to school, my pets and hobbies are all examples of personal details)
- always check with a responsible adult and my parents before I show photographs of myself or friends
- never put a photo of myself online with my school uniform on
- never meet an online friend without taking a responsible adult that I know with me

I understand that:

- once I post a message or an item on the internet then it is completely out of my control
- anything I write or say or any website that I visit may be being viewed by a responsible adult.
- Any inappropriate use will lead to my rights being removed

Signed: *Date:*