ST WENN SCHOOL

Reviewed: July 2020
Date of next Review: July 2021

Headteacher: Mrs Sally Berry

Chair of Governors: Dr Tessa Cubitt:

USE OF THE INTERNET AND DIGITAL DEVICES: ACCESS AND AGREEMENT POLICY

Contents

1. Aims

St Wenn School aims to:

∗ Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors

∗ Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology

∗ Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 Trustees

Governors have overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

Governors will co-ordinate regular meetings with appropriate staff to discuss online safety.

All Governors will:

∗ Ensure that they have read and understand this policy;

∗ Agree and adhere to the terms on acceptable use of the school's IT systems and the internet (appendix 2).

3.2 The Headteacher

∗ Is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

The DSL takes lead responsibility for online safety in school, in particular:

∗ Working with staff, as necessary, to address any online safety issues or incidents;

∗ Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy;

∗ Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy;

∗ Liaising with other agencies and/or external services if necessary.

This list is not intended to be exhaustive.

3.4 The IT Lead (Mr Kevin Beer)

The IT Lead is responsible for:

∗ Ensuring that appropriate filtering and monitoring systems are put in place and maintained, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including 'Prevent' material

∗ Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly;
∗ Ensuring that a security check is carried out monitoring the school's IT systems on a monthly basis;
∗ Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;
∗ Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
∗ Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school;
∗ Ensuring that any online safety incidents are logged and dealt with appropriately inline with this policy;
∗Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:
∗ Maintaining an understanding of this policy;
∗ Implementing this policy consistently;
∗ Agreeing and adhering to the terms on acceptable use of the school's IT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1);
∗ Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy;
∗ Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy;
This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:
∗ Notify a member of staff or the Headteacher of any concerns or queries regarding this policy;
∗ Ensure their child has read, understood and agreed to the terms on acceptable use of the school's IT systems and internet (appendix 1);
Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advicecentre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.7 Visitors and members of the community

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.
In **Key Stage 1**, pupils will be taught to:
∗ Use technology safely and respectfully, keeping personal information private

∗ Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies
Pupils in **Key Stage 2** will be taught to:
∗Use technology safely, respectfully and responsibly
∗ Recognise acceptable and unacceptable behaviour
∗ Identify a range of ways to report concerns about content and contact
*Learn about sources of information - Authentic websites - to avoid 'fake' news
The safe use of social media and the internet will also be covered in other subjects where relevant.
The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our websites. This policy will also be shared with parents.
Online safety will be communicated to parents through written correspondence and the website. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.
Concerns or queries about this policy can be raised with any member of staff.
IT lead runs termly workshops for parents

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school anti-bullying policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the vITim.
The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their classes, and the issue will be addressed in assemblies.
Teachers are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying.
This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).
St Wenn school will send information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.
In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete

inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.
When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:
* Cause harm, and/or
* Disrupt teaching, and/or
* Break any of the school rules
If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:
* Delete that material, or
* Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
* Report it to the police/ MARU

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.
Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.
Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.
We will monitor the websites visited by pupils, staff, governors, volunteers and visitors (where relevant) to ensure they comply with the above.
More information is set out in the agreements in appendices 1 and 2.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school only if communication is necessary during the school day. They do so at their own risk and phones will be handed in to the office for safekeeping at the beginning of the school day and returned at the end of the school day.
They are not permitted to use them during the school day including:
* Lessons
* During Playtime or Lunchtime
* At Clubs before or after school, or any other activities organised by the school
Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).
Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

Staff members using a work device outside school must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2
Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.
If staff have any concerns over the security of their device, they must seek advice from the IT Lead.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.
Where a staff member misuses the school's IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.
All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).
The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
Volunteers will receive appropriate training and updates, if applicable.
More information about safeguarding training is set out in our Safeguarding Policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.
This policy will be reviewed at least every three years. At every review, the policy will be shared with governors.

13. Links with other policies

This online safety policy is linked to our:
* Child Protection and Safeguarding Policy
* Positive Behaviour Policy/ Anti-Bullying Policy
* Staff Code of Conduct Policy
* Complaints procedure
* Managing allegations against other pupils
* Equality and Diversity Policy
* Whistleblowing Policy
* Mobile Phone Policy
* Social Networking Policy

Use of the Internet and Digital Device agreement
Pupils and parents/carers

Name of pupil:

When using the school's IT systems and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the school's network using someone else's details
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during the school day without a teacher's permission. When not in use, my teacher will hold the device securely until the end of the day
- I agree that the school will monitor the websites I visit
- I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others

Signed (pupil): Date:

Parent/carer agreement: I agree that my child can use the school's IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's IT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date:

Use of the Internet and Digital Device Agreement
Governors, staff and volunteers

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, Virtual Learning Environment etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will be professional in my communications and actions when using school IT systems:
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in accordance with the school's policy.

- I will only use mobile phones – both work and personal - in accordance with the school's policy.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school
- When I use my personal mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules/policy set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school's IT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school / academy policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and RestrITed data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work

- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that I am responsible for my actions in and out of the school.
- I will not take or record images of pupils for their personal use; record virtual lessons or meetings using personal equipment (unless agreed and risk assessed by senior staff) or engage online while children are in a state of undress or semi-undress
- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.

In addition to the above, when using technology for online/virtual teaching

- When using the internet for 'virtual teaching' I will check the background - no photos, artwork, identifying features, mirrors – ideally the backing should be blurred.
- I will check that the pupils and I are in living / communal areas – no bedrooms
- I will be fully dressed at all times
- I will not contact pupils outside the operating times defined by the Headteacher to be between 8.30am and 6.30pm
- When selecting a platform, I will check that the provider has an appropriate level of security
- I will ensure that the Headteacher is aware of any meeting taking place and I will not carry our meetings in a one to one situation
- I will not record sessions unless I have a prior agreement to do this with the Headteacher

I understand that if I fail to comply with this 'Use of the Internet and Digital Device Agreement', I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.
I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Governor/Volunteer Name: .....
Signed: .....
Date: .....

Appendix 3: online safety training needs – self-audit for staff
Online safety training needs audit

Name of staff member/volunteer:
Date:

Do you know the name of the person who has lead responsibility for online safety in school?

Do you know what you must do if a pupil approaches you with a concern or issue?

Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?

Are you familiar with the school's acceptable use agreement for pupils and parents?

Do you regularly change your password for accessing the school's IT systems?

Are you familiar with the school's approach to tackling cyber-bullying?

Are there any areas of online safety in which you would like training/further training? Please
record them here:

Signature: