The Federation of Boskenwyn & Germoe Schools

and Nysgerrig Kindergarten

A love of learning for life

NYSGERRIG KINDERGARTEN
AND FOREST SCHOOL

Germoe Community
Primary School

BOSKENWYN
SCHOOL

Acceptable Use and Online Safety policy

This policy was written in September 2022 and reviewed in September 2023. It will, be reviewed annually.

CONTENTS

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, trustees 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, including mobile and smart technology (which we refer to as 'mobile phones')
- 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 (DFE's) statutory safeguarding, keeping children safe in education and is advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyberbullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DFE'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
The policy also takes into account the national Curriculum computing programme of study

3.Roles and responsibilities

3.1. the headteacher
The headteacher is responsible for ensuring that staff understand this policy and that it is being implemented consistently throughout the school.

3.2 The designated safeguarding lead
Details of the schools designated safeguarding lead (DSL) and deputy/deputies are set out in our schools child protection and safeguarding policies as well as relevant job descriptions.

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

- Helping to ensure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the ICT manager and other staff as necessary to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the schoolchild protection policy
- Ensuring that any online safety incidents are logged on MyConcern and dealt with appropriately in line with the school behaviour policy
- Ensuring that any incidents of cyber-bullying are logged on MyConcern and dealt with appropriately in line with the school behaviour policy

- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to governors.

This list is not intended to be exhaustive

3.3 the ICT manager

ICT4 provide IT support and are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the schools ICT systems are secure and protected against viruses and malware and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the schools ICT systems on an hourly basis and reporting to senior leaders
- Blocking access go potentially dangerous sites and where possible preventing the downloading of potentially dangerous files
- 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 dealt with appropriately in line with the school behaviour policy

3.4 All staff and volunteers

All staff including contractors and agency staff and volunteers are responsible for:

- Maintaining and understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the schools ICT systems and the internet (appendix 3) and ensuring that pupils follow the schools terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriate in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment both online and offline and maintaining an attitude of 'it could happen here'

3.5 Parent

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 term on acceptable use of the schools ICT system's and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and website:

- What are the issues? UK safer internet centre
- Hot topics – Childnet International

- Parent resource sheet – Childnet International

3.6 Visitors and members of the community

Visitors and members of the community whose the schools ICT 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 3)

4 Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

Primary schools

In Key Stage 1 pupils will be taught to:

- Use technology safety 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 and 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 concern about content and contact

By the end of primary school pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face to face relationships including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts including online whom they do not know)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary teaching about safeguarding including online safety will be adapted for vulnerable children and victims of abuse and some pupils with SEND

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 website. This policy will also be shared with parents.

6.Cyber-bullying

- 6.1 Definition

Cyber-bullying take 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 1 person or group by another person or group where the relationship involves an imbalance of power. (see also the school behaviour 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 knowhow they can report any incidents and are encouraged to do so including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils explaining the reasons why it occurs the forms it may take and what the consequence can be, Teachers will discuss cyber-bullying with their tutor groups.

Teaching staff 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.
The school has a website "online safety" section where information can be found for 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 specific incident of cyber-bullying the school will follow the process set out in the schools 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.

6.3 examining electronic devices

The Headteacher and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic devices thar they have reasonable grounds for suspecting risk to others.

They may confiscate the device and report the incident to the DSL (or the equivalent) immediately who will decide what to do next. The DSL will make the decision in line with the DFE's latest guidance on screening, searching and confiscation.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation.
- Our behaviour policy

Any complains 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 schools ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the schools term on acceptable use if relevant.

Use of the schools 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 visitor by pupils staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 3.

8.Pupils using mobile devises in school

Primary school

Pupils who bring mobile devices into school will need to hand them into the class teacher on arrival, unless needed for medical reasons or specifically directed by the teacher to use them and under their supervision.

Any use of mobile devices in school by pupils must be inline with the acceptable use agreement (see appendices 1 and2)

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 of school

All staff members will take appropriate seps to ensure their devices remain secure. This includes but is not limited to:

- Keeping the device password protected – strong passwords are at least 8 characters with a combination of upper and lower case, numbers and special characters (eg asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate the schools terms of acceptable use, as set out in appendix 3

Work devices must be used solely for work activities

If staff have any concerns over the security of their device they must seek advice from ICT4.

10.How the school will respond to issues of misuse

Where a pupil misuses the Schools ICT systems or internet, we will follow the procedures set out in our policies on behaviour and internet acceptable use policies. The action taken will depend on the individual circumstances, nature of seriousness of the specific incident and will be appropriate. Parents will be informed, Where a staff member misuses the schools ICT system's 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 /staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents should be reported to the police.

11.Training

All new staff members will receive training as part of their induction on safer internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation through their compulsory safeguarding training.
All staff member 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)

By way of this training all staff will be made aware that:

- Technology is a significant component in any safeguarding and wellbeing issues and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, harassing and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images/or videos especially around chat groups
  - Sharing of abusive images and pornography to those who don't want to receive such content.

Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weight up the risks
- Develop the ability to influence pupils to make the healthiest long term choices and keep them safe from harm in the short term

The DSL 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 and disseminate updates regularly,

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 child protection and safeguarding policy

12.Monitoring arrangements

This policy will be reviewed every year by staff and governors

13.Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

Acceptable use of the schools ICT systems and internet agreement for pupils and parents/carers

Name of pupil...

When I use the schools ICT systems 9like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has old me or allowed me to use
- Tell my teacher immediately if
    - I click on a website by mistake
    - I receive messages from people I don't know
    - I find anything that may upset or harm me or my friends
- Use school computers for schoolwork only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone including my friends
- Never give my personal information (my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules

Signed (pupil)……………………………….. Date……………………………….

Parent/carer agreement: I agree that my child can use the schools ICT systems and Internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the schools ICT systems and internet and will make sure my child understands these
Signed (parent/carer)……………………….. Date………………………………..

Appendix 2 KS2 acceptable use agreement (pupils and parents/carers)

Acceptable use of the schools ICT systems and internet agreement for pupils and parents/carers

Name of pupil...

I will read and follow the rules in the acceptable use agreement policy
When I use the schools ICT systems (like computers) and get onto the internet in school I will:

- Always use the schools ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present or with a teachers permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address ort telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset distress or harm me or others
- Always log off or shut down a computer when I've finished working on it

I will not:
Access any inappropriate websites including social networking sites chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
Open any attachments in emails or follow any links in mails without first checking with a teacher
Use any inappropriate language when communicating online including in emails
Log into the schools network using someone else's details

If I bring a personal mobile phone or other personal electronic device into school
I will not use it during lessons, clubs or other activities organised by the school without a teachers permission
I will use it responsibly and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules

Signed (pupil)... Date..............................

Parent/carer agreement: I agree that my child can use the schools ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the schools ICT systems and internet and for using personal electronic devices in school and will make sure my child understands these
Signed (parent/carer)............................ Date......................................

Appendix 3: acceptable use agreement (staff, governors, volunteers, and visitors)

Acceptable use of the schools ICT systems and internet agreement for staff, governors, volunteers, and visitors

Name of staff member governors, volunteers, and visitors

……….

When using the schools ICT systems and accessing the Internet in school or outside school on a work device (if applicable) I will not;

- Access or attempt to access inappropriate material including but not limited to material of a violent criminal pornographic nature (or create, share link to or send such material)
- Use them in any way which could harm the schools reputation
- Access social networking site or chat rooms
- Use any improper language when communicating online including in emails or other messaging services
- Install any unauthorised software or connect unauthorised hardware or devices to the schools network
- Shae my password with others or log into the schools network using someone else's details
- Take photographs of pupils without checking with teachers firs
- Share confidential information about the schools pupils or staff or the members of the community
- Access modify or share data I'm not authorised to access modify or share
- Promote private business unless that business is directly related to the school

I will only use the schools ICT systems and access the internet in school or outside school on a work device for educational purposes or for the purpose of fulfilling the duties of my role

I agree the school will monitor the websites I visit and my use of ethe schools ICT facilities and systems

I will take all reasonable steps to ensure that work devices are secure an password protected when using them outside school and keep all data securely stored in accordance with this policy and the schools data protection policy

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset distress or harm them or others and will also do so if I encounter any such material

I will always use the schools ICT systems and internet responsibly and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor)……………………………………………

Date………………………………