



*Learning for Life*

# **Fawbert & Barnard's Primary School**

## **Online Safety Policy**

Ratified by Governors:      October 2022

Review Date:                      October 2025

## Contents

1. Aims .....	3
2. Legislation and guidance .....	3
3. Roles and responsibilities .....	3
4. Educating pupils about online safety .....	5
5. Educating parents about online safety .....	6
6. Cyber-bullying .....	6
7. Acceptable use of the internet in school.....	8
8. Pupils using mobile devices in school .....	8
9. Staff using work devices outside school.....	8
10. How the school will respond to issues of misuse .....	8
11. Training.....	9
12. Monitoring arrangements.....	9
13. Links with other policies.....	9
14. Appendix 1: Staff/ governors and volunteers terms on acceptable use.....	11
15. Appendix 2: Pupils terms on acceptable use .....	12
16. Appendix 3: Reporting online safety- concerns .....	13

---

## 1. Aims

Our 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, including mobile and smart technology (which we refer to as 'mobile phones and tablets')
- › Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

### The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- › **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- › **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- › **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- › **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

## 2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- › [Teaching online safety in schools](#)
- › [Preventing and tackling bullying](#) and [cyber-bullying: 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](#). 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.

This policy complies with our funding agreement and articles of association.

## 3. Roles and responsibilities

### 3.1 The governing body

The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

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 ICT systems and the internet (appendix 1)
- › Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures
- › Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

### **3.2 The headteacher**

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**

Details of the school's designated safeguarding lead (DSL) (and deputies) are set out in our child protection and safeguarding policy as well as relevant job descriptions.

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

- › In ensuring 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 school child protection policy
- › Ensuring that any online safety incidents are logged (see appendix 3) 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
- › Providing regular reports on online safety in school to the governing body

This list is not intended to be exhaustive.

### **3.4 The ICT manager**

The ICT manager is 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 school's 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 school's ICT systems on a regular basis
- › Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- › Ensuring that any online safety incidents are logged (see appendix 3) 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.

### 3.5 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 ICT systems and the internet (appendix 1), and ensuring that pupils follow the school's terms on acceptable use (appendix 2)
- › Working with the DSL to ensure that any online safety incidents are logged (see appendix 3) 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
- › 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'

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 ICT systems and internet (appendices 1 and 2)

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

- › What are the issues? – [UK Safer Internet Centre](#)
- › Hot topics – [Childnet International](#)
- › Parent resource sheet – [Childnet International](#)

### 3.7 Visitors and members of the community

Visitors and members of the community who use the school's 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 1).

## 4. Educating pupils about online safety

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

The text below is taken from the [National Curriculum computing programmes of study](#).

It is also taken from the [guidance on relationships education, relationships and sex education \(RSE\) and health education](#).

All schools have to teach:

- › [Relationships education and health education](#) in primary schools
- › [Relationships and sex education and health education](#) in secondary schools

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

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, 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.

Online safety will also be covered during parents' evenings.

The school will let parents know:

- › What systems the school uses to filter and monitor online use
- › What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

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 or the headteacher.

## 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 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 know how 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 consequences can be. Class teachers will discuss cyber-bullying with their classes.

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 (Wellbeing) 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).

The school also sends 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

### **6.3 Examining electronic devices**

The headteacher, and any member of staff authorised to do so by the headteacher (as set out in the behaviour policy) can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff and/or pupils
- Is identified in the school rules as a banned item for which a search can be carried out
- Is evidence in relation to an offence

Before a search, the authorised staff member will:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm,
- Undermine the safe environment of the school or disrupt teaching,
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person

- › The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- › **Not** view the image
- › Confiscate the device and report the incident to the DSL (or 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](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

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

- › The DfE's latest guidance on [searching, screening and confiscation](#)
- › UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- › The school behaviour policy

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 ICT systems and the internet (appendices 1 to 3). 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, 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 to 3.

## 8. Pupils using mobile devices in school

Pupils are not allowed to use mobile devices on site at any point. This includes: during the school day, after school on school site and during any school events e.g. discos or after school clubs.

## 9. Staff using work devices outside school

All staff members will take appropriate steps 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 letters, numbers and special characters (e.g. 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 left inactive for a period of time
- › Not sharing the device among family or friends
- › 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 school's terms of acceptable use, as set out in appendix 1.

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 the ICT Manager.

## 10. How the school will respond to issues of misuse



Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour. 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 ICT 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/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 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).

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

- Technology is a significant component in many 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 and/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 weigh 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 (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 where appropriate.

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

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 3.

This policy will be reviewed every three years by the headteacher or when appropriate. At every review, the policy will be shared with the governing body.

## 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: Acceptable Use Agreement: Staff, Governors and Visitors**  
**Acceptable Use Agreement / Code of Conduct**

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Staff should always aim to ensure data and its usage is done correctly following the GDPR policies. Any concerns or clarification should be discussed with the Headteacher or the computing leader.

I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body

I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities

I will ensure that all electronic communications with pupils and staff are compatible with my professional role

I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to pupils

I will only use the approved, secure email system(s) for any school business

I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick

I will not install any hardware or software without permission of the Headteacher

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory

Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy

Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher

I will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community'

I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher

I will respect copyright and intellectual property rights

I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute

I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies

I will not use personal electronic devices (including smart watches) in public areas of the school between the hours of 8.30am and 3.30pm, except in the staff room

I will ensure to report any breach of data being released incorrectly to the GDPR lead

I will not take any unprotected data home

I will check with the head/ GDPR lead before giving data out to any third party or parent/guardian

I understand this forms part of the terms and conditions set out in my contract of employment

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature ..... Date .....

Full Name ..... (printed)

Job title .....

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

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers	
Name of pupil:	
<p>When using the school's ICT systems and accessing the internet in school, I will not:</p> <ul style="list-style-type: none"><li>• Use them for a non-educational purpose</li><li>• Use them without a teacher being present, or without a teacher's permission</li><li>• Access any inappropriate websites</li><li>• Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)</li><li>• Use chat rooms</li><li>• Open any attachments in emails, or follow any links in emails, without first checking with a teacher</li><li>• Use any inappropriate language when communicating online, including in emails</li><li>• Share my password with others or log in to the school's network using someone else's details</li><li>• Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer</li><li>• Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision</li></ul> <p>If I bring a personal mobile phone or other personal electronic device into school:</p> <ul style="list-style-type: none"><li>• I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission</li><li>• I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online</li></ul> <p>I agree that the school will monitor the websites I visit.</p> <p>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.</p> <p>I will always use the school's ICT systems and internet responsibly.</p>	
Signed (pupil):	Date:
<p><b>Parent/carer agreement:</b> I agree that my child can use the school's 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 school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.</p>	
Signed (parent/carer):	Date:



Learning for Life

Fawbert & Barnard's Primary School

Headteacher: Sue Spearman

Dear Parents

Use of computers in school – Network and Internet including Its learning

As part of our curriculum, we provide a Local Area Network (LAN) where pupils store their computer work and supervised access to the Internet. In line with Government guidelines, we have a Pupil/Home agreement form for pupils and parents/carers to sign to agree to our Acceptable Use policy.

We recognise that using the Internet in school offers access to a wealth of valuable information and activities and the opportunity to send email messages. Unfortunately there is also a risk of accessing unacceptable material. We believe that the benefits to pupils through access to the Internet in the form of information resources and opportunities for collaboration far exceed any disadvantages. Parents and Carers should be aware that every effort has been taken to ensure unacceptable materials are filtered out through the use of tested sophisticated filtering software. Pupils are made aware of what to do should they access any unacceptable material.

During school, teachers will guide pupils towards appropriate materials. Outside school, families bear the same responsibility for such guidance concerning the use of Internet information sources; this can be compared to guidance concerning television, telephones, films, radio, magazine and other potentially offensive media materials.

Alongside the cloud, the school has its own website. Both will enable us to display pupils' work. The enclosed form also requests permission for such display.

We would be grateful if you would read and discuss the Rules of Use with your child, then complete and return the enclosed form.

Yours sincerely

Sue Spearman  
Headteacher

Appendix 3: Reporting Online safety



**Fawbert and Barnard's Primary School**

*Learning for life*

**Online Safety Reporting Concerns Form (OS Form)**

Please complete and alert the Safeguarding Leads or the Computing Subject Leader asap.

**Safeguarding Lead Actions/ Subject Leaders Actions:-**

Date:		Time:		Name of Member of staff reporting:	
Child/Children involved:					
DOB:					
Nature of the incident:	Accidental access to inappropriate materials <input type="checkbox"/>	Intentional access to inappropriate materials <input type="checkbox"/>	Cyberbullying <input type="checkbox"/>	Grooming <input type="checkbox"/>	Other <input type="checkbox"/>
Details:					
The event occurred:	During a lesson <input type="checkbox"/>	Break/lunchtime <input type="checkbox"/>	Afterschool club <input type="checkbox"/>	Outside school hours <input type="checkbox"/>	
Does this warrant police involvement:	Grooming <input type="checkbox"/>	Violent Images <input type="checkbox"/>	Pornographic Images <input type="checkbox"/>	Other <input type="checkbox"/>	
RE STAFF	Family Operations	Actions	COG notified	Actions	
	HR	Actions	Police notified	Actions	
	Details/Reasons for <u>actions:-</u>				
RE CHILDREN	Parents contacted	Actions	Police notified	Actions	
	Details/Reasons for <u>actions:-</u>				



