

Bonnygate Primary School

Online Safety Policy

Agreed by Governors: Tim McSweeney

Date: January 2024

Next Review: January 2025

Bonnygate Primary School

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	5
6. Cyber-bullying	5
7. Acceptable use of the internet in school	7
8. Pupils using mobile devices in school	7
9. Staff using work devices outside school	7
10. How the school will respond to issues of misuse	7
11. Training	8
12. Monitoring arrangements	8
13. Links with other policies	8
Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)	9
Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers)	10
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)	10
Appendix 4: online safety training needs – self-audit for staff	12
Appendix 5: online safety incident report logError! Bookmark ı	not defined.

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')
- 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, <u>Keeping Children Safe in Education</u>, and its advice for schools on:

- <u>Teaching online safety in schools</u>
- 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 board

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

The governing board 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).

The governor who oversees online safety is Tim McSweeney.

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 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college 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:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, 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 on CPOMs 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
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and/or governing board
- This list is not intended to be exhaustive.

3.4 The ICT manager/Trust ICT Team

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 monthly 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 on CPOMs 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 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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? <u>– UK Safer Internet Centre</u>

- Hot topics <u>– Childnet International</u>
- Parent resource sheet <u>– Childnet International</u>

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 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

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

In Key Stage 2, pupils 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 or weekly Newsletter. This policy will also be shared with parents.

Online safety will also be covered during workshops.

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. Teachers will discuss cyber-bullying with their class.
- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. 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).
- 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, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence
- Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:
- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher / DSL / SLT.
- 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, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence
- If inappropriate material is found on the device, it is up to the DSL / Headteacher / 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, and/or
- 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 seminude 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 <u>screening</u>, <u>searching and</u>
<u>confiscation</u> and the UK Council for Internet Safety (UKCIS) guidance on <u>sharing nudes and semi-nudes</u>: <u>advice</u>
<u>for education settings working with children and young people</u>

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

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on <u>sharing nudes and semi-nudes</u>: <u>advice for education settings working with children and young people</u>
- Our behaviour policy / searches and confiscation 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 may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Clubs before or after school, or any other activities organised by the school
- They are to be kept securely in the school office.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

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

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 three words, 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
- 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 school's 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 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 Osborne Co-Operative Academy ICT and internet acceptable use. 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 Osborne Co-Operative Academy Acceptable Use Policy and 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. 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 5.

This policy will be reviewed every year by the Deputy Headteacher. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

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

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers) Osborne Co-operative Academy Trust Foundation Stage & Key Stage 1 Primary Pupils

Osborne Co-operative Academy Trust is a multi-academy trust (MAT) incorporated around the principles and values of the international co-operative movement. These are Equality, Equity, Democracy, Self-help, Self-Responsibility and Solidarity, along with the ethical values of openness, honesty, social responsibility and caring for others. These values and principles underpin all our actions.

EYFS/KS1 Pupil Acceptable Use

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I
 have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I will only send friendly and polite messages
- I know that if I break the rules, I might not be allowed to use a computer / tablet



Appendix 2: KS2 acceptable use agreement (pupils and parents/carers) Osborne Co-operative Academy Trust Acceptable Use of ICT Policy: Key Stage 2 Primary Pupils

Osborne Co-operative Academy Trust is a multi-academy trust (MAT) incorporated around the principles and values of the international co-operative movement. These are Equality, Equity, Democracy, Self-help, Self-Responsibility and Solidarity, along with the ethical values of openness, honesty, social responsibility and caring for others. These values and principles underpin all our actions.

This acceptable user policy refers to the Trust e-Safety Policy, please refer to this for further details.

Responsible Use of the Internet Rules for Key Stage 2 Pupils

The computer system is owned by Osborne Co-operative Academy Trust, and may be used by pupils to further their education and prepare them for today's world. The rules will keep everyone safe and help us to be fair to others.

Pupils requesting Internet access should sign a copy of this Acceptable Internet Use Statement and return it to the Headteacher for approval. Irresponsible use may result in the loss of device/IT equipment access and further penalties.

- 1. I will only use school computers and technology for schoolwork and homework and will use the Internet where it is appropriate and as directed;
- 2. I will not bring files into the school without permission or upload inappropriate material to my workspace;
- 3. I will only edit or delete my own files and not view, or change, other people's files without their permission;
- 4. I will only communicate/message/comment with people I know, or those approved by my teachers and I will write E-mails carefully and politely, in the knowledge that these are monitored by the school;
- 5. I will keep my username and password safe and secure I will not share it, 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;
- 6. I will not open attachments, or download a file, unless I have permission;
- 7. I will not give my home address, phone number, send photographs or video, or give any other personal information that could be used to identify me, my family or my friends;
- 8. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room;
- 9. If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but bring it to the attention of a teacher / trusted adult;
- 10. I should ensure that I have permission to use the original work of others in my own work
- 11. Where work is protected by copyright, I will not try to download copies (including music and videos)
- 12. When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- 13. I will not use the school ICT systems for private purposes;

- 14. I am aware that some websites and social networks have age restrictions and I will respect this;
- 15. I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.
- 16. I will not damage, disable or otherwise harm the operation of the computers or other ICT device sand I will report immediately any damage or faults involving equipment or software.
- 17. I understand that the school will monitor my use of the systems, devices and digital communications.
- 18. I will not use the school systems or devices for on-line gaming, on line gambling, internet shopping, file sharing, or video broadcast

The Trust may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of e-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

Monitoring, Evaluation and Review

The Trust board will review this policy at least every two years and assess its implementation and effectiveness. The policy will be promoted and implemented throughout the school.

Pupil:	Class:

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in
 incidents of inappropriate behaviour, that are covered in this agreement, when I am out of
 school and where they involve my membership of the school community (examples would
 be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.

I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Signed:	Date:

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors) Osborne Co-operative Academy Trust

Responsible use of ICT Acceptable User Policy (Staff & Volunteers)

Staff Name:	Role:
Place of work:	

- I have read and understand the Osborne Co-operative Academy Trust Rules for the responsible use of ICT.
- I agree to abide by all the points above.
- I understand that I have a responsibility for my own and others online safeguarding and I undertake to be a 'safe and responsible digital technologies user'.
- I understand that it is my responsibility to ensure that I remain up to date and read and understand Trust and or schools most recent online safety policies and GDPR related policies.
- I understand that failure to comply with this agreement could lead to disciplinary action.

I understand that I am responsible for my actions in and out of the school:

- 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
- 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.

Signed:	Date:

Please return to your HR manager

Appendix 4: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT		
Name of staff member/volunteer:	Date:	
Question	Yes/No (add comments if necessary)	
Do you know the name of the person who has lead responsibility for online safety in school?		
Are you aware of the ways pupils can abuse their peers online?		
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 ICT 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?		