



ASPIRATIONS

Online safety policy

BOVINGTON ACADEMY

Version control	
April 2025	Reference to Regional CEO changed to Academy Improvement Director References to appendix 3 and 5 removed
April 2023	Role of governors updated 6.3 Updated inline with DfE guidance on searching, screening and confiscation 11 Updated to reflect KCSiE 22
April 2021	Updated to reflect revised AUPs
April 2020	New template

Date of next review:	April 2027	Owner:	Trust Safeguarding Lead
Type of policy:	Outline template	Approval level:	EOB

Contents

1. Aims	2
2. Legislation and guidance	2
3. Roles and responsibilities	3
4. Educating pupils about online safety	4
5. Educating parents about online safety	6
6. Cyber-bullying	6
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 academy will respond to issues of misuse	8
11. Training	8
12. Monitoring arrangements	8
13. Links with other policies	8
Appendix 1: online safety training needs – self audit for staff	9
Appendix 2: online safety incident report log	10

1. Aims

Our academy 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 academy 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 (DfE) 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 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.

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

3. Roles and responsibilities

3.1 The Regional governing board

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

The Academy's Improvement Director and Trust's Director of Safeguarding (both members of the RGB) will ensure the academy holds regular meetings with appropriate staff to discuss online safety, and monitors online safety logs as provided by the designated safeguarding lead (DSL). Online safety will be a focus for monitoring at least twice per year.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the academy's ICT systems and the internet
- 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 principal

The principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the academy.

3.3 The designated safeguarding lead

Details of the academy's DSL and Deputy DSLs are set out in our safeguarding and child protection policy as well as relevant job descriptions.

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

- Supporting the principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the academy
- Working with the principal, ICT lead and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the Safeguarding and Child Protection policy
- Ensuring that any online safety incidents are logged (see appendix 2) 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 academy behaviour policy
- Updating and delivering staff training on online safety (appendix 1 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 principal

This list is not intended to be exhaustive.

3.4 The ICT lead

The ICT lead is responsible for:

- Ensuring there are appropriate filtering and monitoring systems in place, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the academy'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 academy'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 (see appendix 2) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy 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 academy's ICT systems and the internet, and ensuring that pupils follow the academy's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 2) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy behaviour policy

This list is not intended to be exhaustive.

3.6 Parents/Carers

Parents/carers are expected to:

- Notify a member of staff or the principal of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the academy's ICT systems and internet

Parents/carers 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 factsheet - [Childnet International](#)

3.7 Visitors and members of the community

Visitors and members of the community who use the academy'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.

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

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
- 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.

The academy 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/carers about online safety

The academy will raise parent/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

Online safety will also be covered during parent/carers' evenings.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the principal and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the principal.

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 academy 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 academy 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, and the issue will be addressed in assemblies.

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 (see section 11 for more detail).

The academy 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 academy will follow the processes set out in the academy behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the academy 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 Principal, and any member of staff authorised to do so by the Principal, 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 Principal.
- 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 Principal 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 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](#)

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 academy 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 academy's ICT systems and the internet. Visitors will be expected to read and agree to the academy's terms on acceptable use if relevant.

Use of the academy'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).

8. Pupils using mobile devices in school

Pupils are encouraged not to bring mobile devices into the academy, and are not permitted to use them at any point during the school day, including clubs before and after school.

Where parents/carers feel it is vital that their child brings a mobile phone into school, it must be switched off and stored securely. The academy will not take responsibility for any mobile phone that goes missing on school premises unless they are handed into the school office where they will be securely locked away.

Any use of mobile devices in the academy by pupils must be in line with the acceptable use agreement.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the academy 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 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
- Any USB devices containing data relating to the academy must be encrypted, however all staff are encouraged to save data using a cloud based system such as Google rather than a USB 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.

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

Work devices must be used solely for work activities.

10. How the academy will respond to issues of misuse

Where a pupil misuses the academy's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and 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 academy'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. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The academy 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 safeguarding and child protection policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. This policy will be reviewed every 2 years by the Trust Safeguarding Lead. At every review, the policy will be shared with the regional governing board.

13. Links with other policies

This online safety policy is linked to our:

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

Appendix 1: 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?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the academy's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the academy's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the academy's ICT systems?	
Are you familiar with the academy's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 2: online safety incident report log (also record on Arbor)

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident

EYs & KS1 Acceptable Use Agreement

My name is _____

1. To stay **SAFE online and on my devices**,
2. I only **USE** devices or apps, sites or games if a trusted adult says so
3. I **ASK** for help if I'm stuck or not sure
4. I **TELL** a trusted adult if I'm upset, worried, scared or confused
5. If I get a **FUNNY FEELING** in my tummy, I talk to an adult
6. I look out for my **FRIENDS** and tell someone if they need help
7. I **KNOW** people online aren't always who they say they are
8. Anything I do online can be shared and might stay online **FOREVER**
9. I don't do **DARES AND CHALLENGES** just because someone tells me I have to
10. I don't change **CLOTHES** or get undressed in front of a camera
11. I always check with my adult before **SHARING** personal information
12. I am **KIND** and polite to everyone

My trusted adults are:

_____ at school

_____ at home

KS2 Acceptable Use Agreement

These statements can keep me and others safe & happy at school and home

1. ***I learn online*** – I use the school's internet, devices and logons for schoolwork, homework and other activities to learn and have fun. All school devices and systems are monitored, including when I'm using them at home. When e-mailing in school, I will only use my class or school e-mail address.
2. ***I behave the same way on devices as face to face in the classroom, and so do my teachers*** – If I get asked or told to do anything that I would find strange in school, I will tell another teacher.
3. ***I ask permission*** – At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.
4. ***I am creative online*** – As well as looking at things from other people on apps, sites and games, I also get creative to learn and make things, and I remember my Digital 5 A Day.
5. ***I am a good friend online*** – I won't share or say anything that I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.
6. ***I am not a bully*** – I know just calling something banter doesn't make it ok as it could become bullying. I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
7. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
8. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
9. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
10. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
11. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about.
12. ***I know online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
13. ***I check with a parent/carer before I meet an online friend*** the first time; I never go alone.
14. ***I never pretend to be someone else online*** – it can be upsetting or even dangerous.
15. ***I don't do live videos (livestreams) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.

16. ***I don't take photos or videos of people without them knowing or agreeing to it*** – and I never film fights or people when they are upset or angry. Instead ask an adult or help if it's safe.
17. ***I keep my body to myself online*** – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
18. ***I say no when I am online if I need to*** – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
19. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
20. ***I follow age rules*** – 13+ games and apps aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult or skilful but are very unsuitable.
21. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
22. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
23. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour, at home and at school.
24. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
25. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult and/or report it.
26. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
27. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find. If I am not sure I ask a trusted adult.

I have read and understood this agreement.

If I have any questions, I will speak to a trusted adult: at school that includes

Outside school, my trusted adults are _____

I know I can also get in touch with [Childline](#)

Signed: _____

Date: _____