



On-line Safety Policy

Approved by Business Committee	
Ratified by Governing Body	N/A
Owner of Policy - Headteacher	
Date Last Reviewed – 6th March 2024	Next Review by – March 2028

Contents

1. Aims	3
Categories of risk.....	3
2. Legislation and guidance	3
3. Roles and responsibilities.....	5
3.2 The Headteacher	5
3.3 The Designated Safeguarding Lead.....	5
3.4 The ICT manager	6
3.5 All staff and volunteers.....	6
3.6 Parents.....	6
3.7 Visitors and members of the community.....	7
4. Educating pupils about online safety	7
5. Educating parents about online safety	8
6. Cyber-bullying.....	8
6.2 Preventing and addressing cyber-bullying	8
6.3 Examining electronic devices	9
7. Acceptable use of the internet in school	9
8. Pupils using mobile devices in school.....	10
9. Staff using work devices outside school	10
10. How the school will respond to issues of misuse.....	10
11. Training	11
12. Monitoring arrangements	11
13. Links with other policies	12

1. Aims

At Bow School, we acknowledge our responsibility to safeguarding students, staff, volunteers and other stakeholders from the risk of harm that others may present to them or that they may present to themselves both offline and online. We understand our responsibility, therefore, to teach our students, colleagues and stakeholders about how to navigate safely online, how to identify themselves when they may be a risk of harm and how to seek help if they are concerned that they may be at risk.

As we result, we aim 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

This policy should be read in conjunction with other policies, available on our website, such as@

- Bow School Behaviour for Learning Policy
- Bow School Anti-Bullying Policy
- Safeguarding and Child Protection Policy
- ICT Acceptable Use Policy

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, anti-Semitism, 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 scam

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 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

The Education Act 2011 (which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so)

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

3. Roles and responsibilities

3.1 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 through its Health and Safety Committee, Full Governing Body or Link Governance arrangements, it will also monitor online safety as part of the information it receives from the Designated Safeguarding Lead (DSL).

All governors will therefore:

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

Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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 are set out in our Child Protection and Safeguarding Policy.

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 (see appendix 5) 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

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 weekly 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 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

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? – UK Safer Internet Centre
Hot topics – Childnet International
Parent resource sheet – Childnet International
Healthy relationships – Disrespect Nobody

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.

4. Educating pupils about online safety

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

In Key Stage 3, pupils will be taught to:

Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in Key Stage 4 will be taught:

To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
How to report a range of concerns

By the end of secondary school, pupils will know:

Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
What to do and where to get support to report material or manage issues online
The impact of viewing harmful content
That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
How information and data is generated, collected, shared and used online

How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
--

How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)
--

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 virtual learning environment. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings and other parent events.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Designated Safeguarding Lead in the first instance.

Concerns or queries about this policy can be raised with the Designated Safeguarding Lead 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 one 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

This section should be read in conjunction with the school's Anti-Bullying Policy

To help prevent cyber-bullying, we will ensure that pupils understand:

What Cyberbullying is

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. We will seek multi-faceted opportunities to use aspects of the curriculum to cover cyber-bullying. This includes but is not limited to assemblies, tutor-time, House Days, PSHE 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 provides information on cyber-bullying and online safety to parents so that they are aware

of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

Cause harm, and/or
Disrupt teaching, and/or
Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

Delete that material, or
Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

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

The DfE's latest guidance on screening, searching and confiscation
UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
The school's COVID-19 risk assessment

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 1-3). 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 can be found in the school's Acceptable Use of ICT Policy

8. Pupils using mobile devices in school

This section should be read in junction with the school's Behaviour for Learning Policy. In essence:

Pupils may bring mobile devices into school, but:

These should be switched off and placed in bags
--

They should not be seen or heard at any time while the child is on the school site

It should be noted that failure to adhere to the above expectations will lead to these items being **confiscated** in line with the school's Learning Behaviour Policy. The use of Mobile devices in schools will be adapted in accordance to DFE guidelines.

9. Staff using work devices outside school

This section should be read in conjunction with:

Acceptable use of ICT Policy

Staff Code of Conduct

Child Protection and Safeguarding Policy
--

Data Protection Policy

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
--

Installing anti-virus and anti-spyware software

Keeping operating systems up to date – always install the latest updates
--

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

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 school's Network 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 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 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. 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 the risks up
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 their 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

This policy will be reviewed every year by the Designated Safeguarding Lead. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because

technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

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