James Bateman Middle School

Online Safety Policy

Approved by:	Mrs S Maguire
Last reviewed on:	23/03/2023
Next review due by:	23/03/2024

Contents

1. Aims

James Bateman Middle 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

- 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 2022', 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 Trust Board

Trustees have overall responsibility for monitoring this policy and holding schools to account for its implementation. They will review the policy on an annual basis.

3.2 The Governing Board

The governing board also has responsibility for monitoring the school 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 school has a named safeguarding governor who also oversees on-line safety.

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

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 DSL and deputy DSL are set out in our child protection and safeguarding policy as well 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;
- 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 appropriate filtering and monitoring systems, 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 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 (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 2), 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 4) 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.

3.6 Parents

Parents are expected to:

- notify the headteacher, or a member of staff of the appropriate school, 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 factsheet - 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 3).

4. Educating pupils about online safety

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

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 Key Stage 2** 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.

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.

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 (VLE). This policy will also be shared with parents.

The school will let parents know what systems the school uses to filter and monitor online use. The school will tell parents what their children are being asked to do online (e.g. sites they need to visit or who they'll be interacting with online)

Online safety will also be covered during parents' evenings.
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 of the appropriate school.

Concerns or queries about this policy can be raised with the headteacher, or any member of staff of the appropriate school.

6. Cyber- Bullying

6.1 <u>Definition</u>

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 <u>Preventing and addressing cyber-bullying</u>

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/form teachers will discuss cyber-bullying with their tutor groups, 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 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 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 a staff member believes a device may contain a nude or semi-nude image or an image that it's a criminal offence to possess, they will not view the image but will report this to the DSL (or equivalent). The DSL will then decide what to do next, in line with the relevant guidance.

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
- any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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.

Schools 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, 2 and 3.

8. Pupils using mobile devices in school

Each school will adapt this section according to stage and age.

Pupils may bring mobile devices into school, but are not permitted to use them during:

- lessons
- tutor group time
- clubs before or after school, or any other activities organised by the school

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 devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

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

Work devices must be used solely for work activities.

Staff using a personal device such as laptop, tablet or mobile phone should keep data secure either by:

- accessing documents on a secure cloud service such as Office 365
- using an encrypted device
- using an encrypted pen-drive

They should also ensure that:

- documents with personal data are password protected;
- the device is password-protected. They should use a strong password or a PIN to lock devices, to prevent others from accessing data through them. Strong passwords are at least **8 characters**, with a combination of upper and lower-case letters, numbers and special keyboard characters (e.g. an asterisk or currency symbols).

Staff must follow the following advice:

- replace letters with numbers and symbols. For example, replace 'a' with '4'
- don't use personal information such as pet names or nicknames
- don't use common words (e.g. password) or sequences like 1234
- don't re-use passwords

Staff should not share any devices that store personal data among their family or friends.

Antivirus software is installed on laptops and computers which is kept up to date and makes regular scans.

10. How the school will respond to issues of mis-use

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/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.

The DSL and deputy/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 Trust Board. In addition to the latest guidance regarding Internet safety, feedback from the e-Safety co-ordinator (normally the DSL), headteacher and local governing boards will be used to inform any policy review.

13. Links with other policies

This online safety policy will be linked to other school policies:

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

13.1 Useful Links for Parents/Carers

Thinkuknow - a leading site with help for all sorts of users including parents/carers.

Parents Protect - a good detailed site with easy to find articles.

Saferinternet.org - lots of advice on all aspects of e-safety.

Internetmatters.org - a good site for many aspects but especially for setting up controls on devices.

Connectsafely.org - a US based site but with good parental guides on various apps and websites.

Parents are encouraged to visit the family safety information for the operating system/s you are using - for example, for Windows 7 visit: windows.microsoft.com

13.2 Useful links for Schools

Thinkuknow - some resources for teaching e-safety - as a minimum, the e-safety coordinator should join as a teacher user, but all teachers could usefully do so.

Childnet resources - some resources for teaching and a wealth of advice.

Safer Internet Centre - a good range of advice and a helpline.

South West Grid for Learning site - a wealth of resources and a good source of policy advice and templates.

DfE - advice on bullying including cyberbullying.

360-degree safe site - home of the e-safety Mark and a great way to improve practice.

Online Compass - a simple and easy review and improvement tool

Appendix 1

KS2 and KS3

Acceptable use agreement (pupils and parents/carers)

Schools will adapt this agreement to reflect their approach, in line with any changes made to this policy.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

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

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

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

Signed (pupil):	**Date:**

Parent/carer's agreement: 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.

Signed (parent/carer):	**Date:**

Appendix 2

Acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

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

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

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

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

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

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

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3

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 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?	

Appendix 4

Online safety incident report log

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**

Policy Adoption and Revision Details				
Policy Adoption:	LBG	Effective date:	24/03/2022	
Review	March 2023	Review Date:	23/03/2023	Version 1
Review		Review Date:		