



BELLE VUE
GIRLS' ACADEMY

BELLE VUE GIRLS' ACADEMY

E-Safety Policy

Reviewed by	Approved by	Date of Approval	Next Review Date
VDU	LGB	Summer 26/27	Summer 27/28

1. Policy Statement

This policy also reflects the academy's commitment to safeguarding pupils in an increasingly digital world, including emerging technologies such as artificial intelligence, social media platforms and online communication tools.

The ethos of Belle Vue Girls' Academy is based on the need for each member of our school community to give and receive respect. We expect that each member of our community will care for others and will challenge attitudes and behaviours which are not in keeping with these values. We have the same high expectations when working online.

2. 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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Ensure that all members of the school community understand the risks associated with new and emerging technologies, including artificial intelligence and social media platforms
-

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, [Keeping children safe in education 2025](#) ,

It also reflects DfE advice and guidance on:

- [Teaching online safety in schools](#) (DfE, 2023 update)
- [Preventing and tackling bullying](#) (DfE, 2017) and [cyber-bullying: advice for headteachers and school staff](#)
- Relationships, Sex and Health Education (RSHE) statutory guidance (DfE, updated 2025, effective from September 2026) [Relationships and sex education \(RSE\) and health education - GOV.UK](#)
- [Searching, screening and confiscation](#) (DfE updated 2023)
- [Generative artificial intelligence \(AI\) in education - GOV.UK](#) (DfE, updated 2025)
- Education for a Connected World – GOV.UK: Education for a Connected World framework (2020)

It also refers to [protecting children from radicalisation](#) (DfE guidance).

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.

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

3. Roles and Responsibilities

3.1 The Local Governing Body

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

The governing board will monitor online safety incident logs as provided by the designated safeguarding lead (DSL) as part of the 'Safeguarding Report to Governors'.

The governor who oversees Safeguarding, including online safety, is **Nurjahan Ali Arobi** 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 2)

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 deputies are set out in our 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 technician, AIT and other staff, as necessary, to address any online safety issues or incidents
- 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
- Ensuring appropriate safeguarding responses to incidents involving artificial intelligence, online exploitation, misinformation and emerging online risks
- Updating and delivering staff training on online safety
- 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 Our Learning Cloud (BDAT external IT support service)

AIT is responsible for:

- Putting in place appropriate filtering and monitoring systems (currently Securely and Smoothwall or equivalent approved 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
- Ensuring systems meet the DfE filtering and monitoring standards (2023)

- Conducting a full security check and monitoring the school's ICT systems on a routine basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

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 (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy and the Safeguarding Policy
- Maintain an awareness of emerging online risks, including AI-generated content, deepfakes and harmful online trends
-
- 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/Carers

Parents/Carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure that both their child and themselves have read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)
- Report any online incidents/activity in breach of this policy to the school in a timely fashion.
- Support the school in reinforcing expectations around safe use of technology at home, including appropriate use of social media and AI tools
-

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](#)
- Healthy relationships – [Disrespect Nobody](#)

3.7 Students

Students are expected to:

- Ensure they have read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)
- Report any online incidents/activity in breach of this policy to their Tutor, Pastoral Manager, Academic Leader, Teacher or any adult in school in a timely fashion.
- Take responsibility for keeping themselves and others safe online.

- Assess the personal risks of using any particular technology and behave safely and responsibly to limit those risks.
- Understand that misuse of AI tools (e.g. plagiarism, generating inappropriate content) is treated as a breach of academy expectations

3.8 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 2).

Visitors should use the designated guest WiFi network when onsite.

4. Educating Pupils about Online Safety

Pupils will be taught about online safety as part of the curriculum at Belle Vue Girls' Academy.

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
- Understand how to critically evaluate online content, including identifying misinformation, fake news and AI-generated content

• 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
- Understand the ethical use of artificial intelligence and the risks associated with its misuse
- Understand how algorithms, data collection and online platforms influence content and behaviour
- How to report a range of concerns

• In Key Stage 5 (Sixth Form), students will be supported to:

- Develop independence in managing their digital footprint, online identity and reputation
- Critically evaluate online information, including misinformation, bias and AI-generated content
- Understand the risks associated with online relationships, exploitation and coercion
- Use technology, including artificial intelligence, ethically and responsibly in academic work and personal contexts
- Prepare for safe and responsible use of technology in higher education, employment and wider society

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

The safe use of social media and the internet will also be covered as part of the academy's Personal Development Curriculum.

For more information on when and how the areas listed above are covered in our curriculum, please visit the 'Relationships & Sex Education' section of the academy website.

5. Educating Parents about Online Safety

The school will raise parents' awareness of internet safety in newsletters or other communications home, and in information via our website. This policy will also be shared with parents via our website. The school will provide updates on emerging technologies and risks (e.g. AI, new apps, online trends) through newsletters, the website or workshops where appropriate

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with their child's Pastoral Manager or Head of Year.

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

6. Cyber-bullying

This section should be read in conjunction with our academy **Anti-Bullying Strategy** which can be found in section 8 of our **Behaviour and Welfare Policy**, accessible via our website.

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, and may include anonymous or AI-generated abuse

6.2 Preventing and Addressing Cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils are taught through our curriculum (see section 4) to 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. Form Tutors will discuss cyber-bullying with their tutor groups as part of our Personal Development programme and address misuse of technology such as impersonation, fake accounts, and AI-generated harmful content. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying.

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 on cyber-bullying to parents via our newsletter and website, 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

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 & 2). 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. Use of artificial intelligence tools must comply with school expectations and must not be used to produce inappropriate, harmful or dishonest work

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 & 2.

8. Remote Learning & Independent Learning

Belle Vue Girls' Academy's agreed learning platform is Microsoft 365. Students and staff should only communicate with each other for learning purposes using this platform. All students and staff have been trained on the use of Microsoft 365 (or other approved platforms as determined by the school). Use of external platforms or apps for communication between staff and students is strictly prohibited unless authorised

.

When involved in live on-line learning, students and staff should follow the protocols as set out in the [Remote Learning Policy](#)

9. Pupils Using Mobile Devices in School

9.1 Statement of Intent

In response to Department for Education guidance on mobile phones in schools (2024), Belle Vue Girls' Academy has implemented a system to ensure that pupils do not have access to mobile phones throughout the school day, including during lessons, transitions, break times and lunchtime.

As a school we have a duty to create an environment that is calm, safe and free from distraction so all pupils, whatever their background, can learn and thrive. One of the greatest challenges facing schools is the presence of mobile phones. Mobile phones can present unnecessary distraction, disruption and diversion.

Mobile phones now include many additional functions such as an integrated camera, video recording capability, instant messaging, mobile office applications, access to artificial intelligence tools and mobile access to the internet. These allow immediate access to social media, messaging platforms and online content, which can pose risks to safeguarding, wellbeing and learning.

To address these risks, the school has introduced a secure mobile phone pouch system, which ensures that phones are inaccessible during the school day.

9.2 Secure Phone Pouch System

All pupils in Years 7–11 are required to use a school-issued secure mobile phone pouch.

- Upon arrival to school, pupils must place their mobile phone into the secure pouch before entering the main school building.
- Pouches will be locked before pupils move into the main school environment.
- During tutor time, pupils must place their locked pouch on their desk so staff can check that it is securely locked.
- Throughout the school day, pouches must remain locked and stored in the pupil's school bag.
- Pouches may only be unlocked by authorised staff (e.g. Pastoral Team) or at designated unlocking stations at the end of the school day.
- At the end of the day, pupils will unlock their pouches at designated unlocking stations under staff supervision.

Any attempt to tamper with, damage, or bypass the pouch system will be treated as a serious breach of the Behaviour Policy.

9.3 Expectations and Rationale

This system ensures that mobile phones are not used, seen or accessible during the school day.

By removing access to mobile phones, the school aims to:

- Improve focus, behaviour and engagement in lessons
- Reduce incidents of cyber-bullying and online conflict during the school day
- Support positive social interaction and wellbeing
- Minimise safeguarding risks associated with cameras, messaging and online content

9.4 Breach of Policy

If a pupil is found to have access to a mobile phone outside of the secure pouch system, or if the pouch system is not used correctly, this will be treated as a breach of the school's Behaviour Policy.

Sanctions may include confiscation of the device, parental contact, or further disciplinary action depending on the nature and frequency of the incident.

9.5 Sixth Form

Sixth form students are not required to use secure phone pouches.

They may use mobile phones only within the Sixth Form Study Area and in line with staff expectations.

Use of phones in lessons is only permitted where explicitly authorised by the teacher.

Sixth form students are expected to model responsible and appropriate use of mobile devices.

Failure to do so may result in sanctions in line with the Behaviour Policy.

This system replaces previous mobile phone expectations and applies to all pupils in Years 7–11."

10. 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 they use a school device with an encrypted hard drive – 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. The school device should also have up to date anti-virus and anti-spyware software
- Making sure the device is locked if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping operating systems up to date – always install the latest updates
- Not use personal AI tools or applications to process sensitive school data unless approved and compliant with GDPR requirements

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 2, or the BDAT Acceptable use of ICT Policy.

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 Academy Business Leader, who will liaise with AIT.

11. 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 Behaviour & Welfare E-Safety policies. 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 trust's

staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

Incidents involving AI misuse, inappropriate content creation, or digital impersonation will be treated as serious breaches of safeguarding and behaviour policies.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training

All new staff members will receive a copy of this policy as part of their induction and must sign to acknowledge that they have read and understood it. All new staff will receive safeguarding training, which will include 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, ebulletins and staff meetings). Training will include awareness of emerging technologies such as AI, online manipulation, and evolving safeguarding risks.

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 online safeguarding issues as part of their annual safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our safeguarding policy.

13. Monitoring Arrangements

All staff log e-safety incidents on CPOMS and the DSL oversees the log of behaviour and safeguarding issues, including those related to online safety.

Filtering and monitoring systems are reviewed regularly to ensure they remain effective and compliant with DfE standards.

This policy will be reviewed annually by the Deputy Headteacher responsible for Behaviour, Attitudes and Personal Development. At every review, the policy will be shared with the governing board.

14. Emerging Technologies and Artificial Intelligence

The school recognises the rapid development of digital technologies, including artificial intelligence. The academy will proactively review and update its practices to ensure safe, ethical and appropriate use of such technologies by staff and students

15. Links with Other Policies

This online safety policy is linked to our:

- BVGA Safeguarding Policy & Child Protection Policy

- BVGA Relationships, Sex and Health Education Policy
- BVGA Remote Learning Policy
- BVGA Behaviour & Welfare Policy
- BVGA ICT and internet acceptable use policy (appendices 1 & 2)
- BVGA Staff Code of Conduct
- BDAT Staff Disciplinary Procedure Policy
- BDAT Acceptable Use of ICT Policy
- BDAT Social Media Policy
- BDAT GDPR Policy & Privacy Notices
- BDAT Complaints Policy
- Appendix 1: Acceptable use of ICT Agreement (pupils and parents/carers)

*A copy of this is in student data collection packs and must be signed by students and their parents/carers

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

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. Your online area is your responsibility. You cannot claim that 'it must have been someone else'. Get your password changed if you think someone knows (ask your IT teacher).
- 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/carers
- 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
- Always demonstrate good behaviour on the Internet, the same as I would in a classroom or on an academy corridor. I understand that the normal Behaviour Policy and sanctions apply.

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, or share my details with others
- Arrange to meet anyone offline without first consulting my parent/carers, or without adult supervision
- Use artificial intelligence tools to create inappropriate content or submit work that is not my own
- Access or attempt to access my mobile phone or personal electronic device during the school day
- Tamper with, damage or attempt to bypass the school's secure phone pouch system

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

- I will place my phone in the school's secure phone pouch at the start of the school day
- I will ensure the pouch is securely locked before entering the main school building
- I will keep my phone in the locked pouch in my bag throughout the day
- I will not access my device during the school day
- I will only unlock the pouch at the end of the school day or when directed by a member of staff
- I understand that failure to follow this system will result in sanctions in line with the Behaviour Policy
- I understand that my device may be confiscated if the policy is breached

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, including the school's expectations regarding mobile phones and the secure phone pouch system, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 2: Acceptable use of ICT Agreement (staff, governors, volunteers and visitors)

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

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
- Use artificial intelligence tools in a way that breaches confidentiality, safeguarding, or data protection policies

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.

Name: _____ Position: _____

Signed: _____

Date: _____