The Bemrose School

Online Safety Policy

Date of policy publication: September 2025

Author/s of policy: Rebecca Broderick - DSL

Date of last review: July 2025

Date of next review: July 2026

(Please note, further updates maybe required once KCSIE 2025 has been released)

Important contacts:		
Online Safety Link Governor	**Ollie Shearer**	**01332 366711** **jgrant@bemrose.derby.sch.uk**
Online Safety Lead	**Rebecca Broderick DSL**	**01332 366711** **rbroderick@bemrose.derby.sch.uk**
Deputies Online Safety Hub Members	**Ailsa O'Reilly - LD IT** **Martin Rowe Headteacher Secondary** **Phil Wood - Assistant Headteacher PD**	**aoreilly@bemrose.derby.sch.uk** **Mrowe@bemrose.derby.sch.uk** **pwood@bemrose.derby.sch.uk**
Key staff - Online Safety Hub Members	**Harriet Sherwood PSHE Lead [Secondary] Emma Powers PSHE Lead [Primary]**	**hsherwood@bemrose.derby.sch.uk** **epowers@bemrose.derby.sch.uk**

Contents

1. Aims

1.1 Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents, and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support staff in teaching pupils safe and effective internet and ICT use

1.2 The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate, or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending, and receiving explicit images (e.g., consensual, and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Relevant Legislation and Guidance

This policy is based on the Department for Education's (DfE's) 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 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.

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping children safe in education - GOV.UK
- Searching, screening and confiscation: advice for schools
- National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021

3. Roles and responsibilities

3.1 The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Executive Headteacher to account for its implementation.

The Governing Body will co-ordinate termly meetings with the Online Safety lead to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The Governor who oversees online safety is Ollie Shearer**.**

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
- 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 Executive Headteacher

The Executive Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

Details of the school's Designated Safeguarding Lead (DSL) and deputies are set out in our safeguarding policy as well as relevant job descriptions.

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

- Supporting the Executive Headteacher and Heads of school in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Executive Headteacher, ICT Team 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 Safeguarding Policy policy
- Ensuring that any online safety incidents are logged via CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Executive Headteacher and/or governing board
- Ensuring that any online safety incidents are logged via CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Ensuring there is an appropriate level of security protection procedures, such as filtering and monitoring systems (Smoothwall), 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

This list is not intended to be exhaustive.

3.4 The ICT Team

The ICT Team is responsible for:

- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting security checks 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 all users of the school's ICT facilities will have clearly defined access rights to school systems, files, and devices. (These access rights are managed by the school's IT team and LINK ICT).

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, and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL (and DDSL) to ensure that any online safety incidents are logged 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, DSL or the Executive 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

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

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. They will need to sign in via reception using the iPad to confirm acceptance to the terms.

4. Curriculum

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

- The text below is taken from the National Curriculum computing programmes of study.
- It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education, Keeping Children Safe in Education

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

4.1 EYFS

In EYFS, pupils will be taught to:

1. Always tell a grown up when they are using the internet and let them help choose safe websites
2. Always tell a grown up if something you are not expecting comes onto their screen
3. Always tell a grown up if someone they don’t know sends them messages or tires to speak to them on the internet

4.2 Key Stage 1

In **Key Stage 1**, pupils will be taught to:

1. Use technology safely and respectfully, keeping personal information private
2. Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

4.3 Key Stage 2

Pupils in **Key Stage 2** will be taught to:

1. Use technology safely, respectfully, and responsibly
2. Recognise acceptable and unacceptable behaviour
3. Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils should know:

- That people sometimes behave differently online, including by pretending to be someone they are not

- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content, and contact, and how to report them
- How to critically consider their online friendships and sources of information Including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

4.4 Key Stage 3

In **Key Stage 3**, pupils will be taught to:

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

4.5 Key Stage 4

Pupils in **Key Stage 4** will be taught:

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

By the **end of secondary school**, pupils should 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.

4.6 Key Stage 5

Pupils will be taught:

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

By the **end of secondary school**, pupils should 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.

The SENCO is responsible for:

- Advising teaching staff how best to identify and support pupils' individual needs.
- Advising staff on the use of TAs in order to meet pupils' individual needs.
- Advising and adapting content to meet needs
- Arranging smaller group sessions that are contextually appropriate.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Artificial Intelligence (AI)

The Bemrose School acknowledges that generative AI tools can be positive, but it can also be used to produce content that is dangerous, harmful, and inappropriate. Pupils will be taught about the risks of using AI tools and how to use them safely. Pupils will be made aware of how to report any concerns or incidents involving generative AI, and who to talk to about any issues regarding the use of AI tools. The school will regularly inform parents/carers of the safeguarding risks that come with using AI tools, and how the school is protecting pupils online.

Educating parents about online safety

The school will raise parents' awareness of internet safety during parent events (parent evenings or events in the community, in letters or other communications home, and in information via our website or school platform. This policy will also be shared with parents.

We believe it is important to model for pupils, and help them learn how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

Online safety will also be covered during Parents Evening and Target Setting Day for parents and carers.

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

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

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

5. Cyber-bullying

5.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school Behaviour Policy.)

5.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. personal, social, health and economic (PSHE) and IT teachers will discuss cyber-bullying with their classes.

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.

The school also sends information/leaflets/articles in the newsletter on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

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

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

5.3 Examining electronic devices

The Executive Headteacher, and key senior staff 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:

- 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 Executive Headteacher, Head of School or DSL 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 deputies) 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

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6. 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. 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.

7. Acceptable use of school email

The school provides each member of staff with an email address. This email account should be used for work purposes only. Multi-factor authentication is enabled on staff email accounts. All work-related business should be conducted using the email address the school has provided.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed, and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information. If staff send an email in error that contains the personal information of another person, they must inform the IT team and the School Business Manager who will liaise with the DPO in DCC immediately and follow our data breach procedure.

Staff must not share their personal email addresses directly with parents and pupils and must not send any work-related materials using their personal email account. Staff should also not send anything to pupils personal email accounts, only their school accounts.

8. Acceptable use of school phones

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use.

Staff who would like to record a phone conversation should speak to the IT staff and LINK IT along with their line manager.

All non-standard recordings of phone conversations must be pre-approved, and consent obtained from all parties involved.

The recording of a phone conversation can be approved by speaking to your line manager or a member of the Leadership Team. A colleague may wish to record a phone conversation when:

- Discussing a complaint raised by a parent/carer or member of the public
- Calling parents to discuss behaviour or sanctions
- Taking advice from relevant professionals regarding safeguarding, special educational needs (SEN) assessments, etc.
- Discussing requests for term-time holidays

Staff must not give their personal phone numbers to parents or pupils. Staff should use phones provided by the school to conduct all work-related business, where staff are using a personal mobile account staff should hide their personal phone numbers from being displayed when calling for work-related business.

9. Acceptable use of school IT facilities for personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The IT staff or LINK IT may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during [contact time/teaching hours/non-break time]
- Does not constitute ‘unacceptable use’, as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school’s ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the school’s ICT facilities for personal use may put personal communications within the scope of the school’s ICT monitoring activities. Where breaches of this policy are found, disciplinary action may be taken.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents could see them.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's policy on the school premises or accessing the schools IT systems.

10. Social Media

10.1 Personal social media accounts

Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Twitter accounts see Staff Code of Conduct Policy.

10.2 School social media accounts

The school has an official Twitter page and there are departmental pages managed by the Executive Headteacher or in the case of departmental pages the Learning Director. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

11. Remote access

We allow staff to access the school's ICT facilities and materials remotely.

The school remote system is managed by the IT team and LINK IT. It is secure and password encrypted to access. Staff must log onto the system using their own passwords. If they do not have access and require this, they should contact the IT Team and LINK IT. Information must not be shared remotely.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the IT team or LINK IT may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

12. Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited

- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only staff authorised by DSL (pupil matters) and Executive Headteacher (staff matters) may inspect, monitor, intercept, assess, record, and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures, and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

13. Pupils using mobile devices in school

Pupils in Year 6 are allowed to bring a mobile into school if they walk home from school without an adult. The phone must be handed to the class teacher in the morning where they will keep it safe until the end of the school day.

Pupils from Years 7 to 13 may bring mobile devices into school, but are not permitted to use them during the following, without express permission by the leading member of staff, such as their teacher, other than to check their timetables:

- 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, students are to use BYOD when using personal devices to access the school wireless network.

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. Please refer to The Bemrose School Behaviour Policy.

Pupils must take full responsibility for their own devices. The school is not responsible for the security or transportation of personal devices. These devices must be left on silent mode or switched off.

14. Staff using work devices outside of 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)
- Hard drives on laptops given to staff have already been 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 is locked if left unattended.
- Not sharing the device among family or friends
- Keeping operating systems up to date by always installing the latest updates, this can easily be done by restarting the machine as opposed to shutting it down.
- Staff members must not use the device in any way which would violate the school's terms of acceptable use.
- If using a removable storage device this will need to be bitlocker encrypted.
- If staff have any concerns over the security of their device, they must seek advice from the IT Manager Mark Fryers, or by sending an email to ictsupport@bemrose.derby.sch.uk

15. 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 policy. 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 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.

Consequences for students who fail to adhere to user agreement for mobile phones and other personal devices may include, but are not limited to, the following, either singularly or in combination depending on the individual circumstances:

- Temporary confiscation of device.
- Search of device contents to locate evidence of misuse.

- BSR, parent meetings, community events, suspension, and/or revocation of access privileges to personal and school technology resources.
- Legal action and prosecution by relevant authorities.

16. Cyber Essentials 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 DDSL will undertake 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 policy.

17. Monitoring arrangements

All staff will log behaviours and safeguarding issues related to online safety via CPOMS. CPOMS is monitored by the DSL and the deputies.

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

18. Links with other policies

This online safety policy is linked to our:

- Safeguarding policy
- Behaviour policy
- Staff code of conduct
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1: Definitions

- **“ICT facilities”:** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service
- **“Users”:** anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors, and visitors
- **“Personal use”:** any use or activity not directly related to the users’ employment, study, or purpose
- **“Authorised personnel”:** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **“Materials”:** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs
- **Antivirus** Software designed to detect, stop, and remove malicious software and viruses.
- **Cloud** Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
- **Cyber-attack** An attempt to access, damage or disrupt your computer systems, networks, or devices maliciously.
- **Cyber incident** Where the security of your system or service has been breached.
- **Cyber security** protection of your devices, services, and networks (and the information they contain) from theft or damage.
- **Download attack** Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
- **Firewall** Hardware or software which uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
- **Hack S**omeone with some computer skills who uses them to break into computers, systems, and networks.
- **Malware** Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
- **Patching** Updating firmware or software to improve security and/or enhance functionality.
- **Pentach**ord for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
- **Phishing** Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.
- **Ransomware** Malicious software that stops you from using your data or systems until you make a payment.
- **Smoothwall –** is the platform The Bemrose School uses for filtering and monitoring.
- **Social engineering** Manipulating people into giving information or carrying out specific actions that an attacker can use.
- **Spear-phishing** A more targeted form of phishing where an email is designed to look like it’s from a person the recipient knows and/or trusts.

- **Trojan** A type of malware/virus designed to look like legitimate software that can be used to hack a victim’s computer.
- **Two-factor/multi-factor authentication** Using 2 or more different components to verify a user’s identity.
- **Virus** Programs designed to self-replicate and infect legitimate software programs or systems.
- **Virtual Private Network (VPN)**An encrypted network which allows remote users to connect securely.
- **Whaling** Highly targeted phishing attacks (where emails are made to look legitimate) aimed at senior executives.