E-SAFETY POLICY

Date Approved	2 July 2025
Date of Next Review	July 2027
Author	Deputy Head, SAB
Committee	Pastoral & Community
Locations Published	Internal SharePoint Portal BGS Website

Table of Contents

Introduction

1. This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:
    1. Teaching online safety in schools
    2. Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
    3. Relationships and sex education
    4. Searching, screening and confiscation
    5. It also refers to the DfE's guidance on protecting children from radicalisation.
2. 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.
3. This policy complies with our funding agreement and articles of association.

Roles and Responsibilities

The following section outlines the roles and responsibilities for eSafety of individuals and groups within the school:

The Board of Trustees

1. The Trustees have overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.
2. The Trustees will be briefed by appropriate staff on online safety, and receive updates from the designated safeguarding lead (DSL).
3. All Trustees will:
    1. Ensure that they have read and understand this policy.
    2. Agree and adhere to the terms on acceptable use of the school's ICT systems and the Internet *(Appendix B below)*.

The Headteacher

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

The designated safeguarding lead

1. Details of the school's designated safeguarding lead (DSL) and deputy are set out in our Safeguarding policy.
2. The DSL takes lead responsibility for online safety in school, in particular:
    1. Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
    2. Working with the Headteacher, network manager and other staff, as necessary, to address any online safety issues or incidents.
    3. Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.

4. Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
5. Updating and delivering staff training on online safety.
6. Liaising with other agencies and/or external services if necessary.
7. Providing regular reports on online safety in school to the Headteacher and/or governors.

3. This list is not intended to be exhaustive.

The Network manager is responsible for

1. Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
2. Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
3. Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
4. Conducting a full security check and monitoring the school's ICT systems on an ongoing basis.
5. Working alongside pastoral colleagues to ensure that any online safety incidents (including cyber-bullying) are dealt with appropriately.
6. This list is not intended to be exhaustive.

All staff and volunteers

1. All staff, including contractors and agency staff, and volunteers are responsible for:
    1. Maintaining an understanding of this policy.
    2. Implementing this policy consistently.
    3. Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the Internet, and ensuring that students follow the School's terms on acceptable use *(Appendices A and B below)*.
    4. Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy.
    5. Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
2. This list is not intended to be exhaustive.

Parents/Carers are expected to

1. Notify a member of staff or the Headteacher of any concerns or queries regarding this policy.
2. Ensure their child has read and understood the terms on acceptable use of the school's ICT systems and Internet.
3. Parents can seek further guidance on keeping children safe online from the following organisations and websites:
    1. ThinkUKnow, CEOP.
    2. What are the issues?, UK Safer Internet Centre
    3. ChildNet parents and carers resource sheet
    4. Hot topics, Childnet International

Visitors and members of the community

1. Visitors and members of the community who use the school's ICT systems or the Internet will be made aware of this policy, when relevant, and expected to read and follow it.
2. If appropriate, they will be expected to agree to the terms on acceptable use.

Students

1. Are responsible for using BGS ICT systems in accordance with the Student Acceptable Use Agreement.
2. Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
3. Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
4. Will be expected to know and understand BGS policies on the use of mobile devices. They should also know and understand school policies on the taking / use of images and on cyberbullying.
5. Should understand the importance of adopting good eSafety practice when using digital technologies out of school and realise that the eSafety Policy covers their actions out of school, if related to their membership of the school.

ICT Infrastructure

The School will be responsible for ensuring that the School network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

1. School ICT systems will be managed in ways that ensure that the School meets recommended technical requirements as per best-practice guidelines from our software vendors through ongoing training (e.g. Microsoft).
2. There will be regular reviews and audits of the safety and security of School technical systems, conducted by the Director of ICT Infrastructure and reported to the C&P committee.
3. Servers, wireless systems and cabling must be securely located and physical access restricted.
4. All users will have clearly defined access rights to School ICT systems and devices.
5. All users will be provided with a username and secure password by the network team who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every full term.
6. The administrator passwords for the School ICT system, used by the Network Manager must also be kept in the School's safe.
7. Internet access is filtered for all users. Illegal content is filtered by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and Internet use is to be logged and regularly monitored. Requests for filtering changes are to be made *via* an email to itsupport@bourne-grammar.lincs.sch.uk so that the request can be logged.
8. Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the Internet.
9. The School has differentiated user-level filtering for staff, students and guests.
10. School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Policy.
11. Users are able to report any actual technical problems or security breaches by contacting the Network Team.

12. Appropriate security measures are in place to protect the core network and workstations from accidental or malicious attempts which might threaten the security of the school systems and data. These are updated and tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
13. An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems using filtered WiFi access.
14. Staff are strongly encouraged not to download executable files and install programs on school laptop computers and mobile devices. Any colleague wishing to do so should take advice from a Network Team colleague before attempting to do so.
15. Personal data must not be sent over the Internet or taken off the school site unless safely encrypted or otherwise secured (e.g. on a school-issued laptop), in accordance with the Data Protection policy. The School provides a secure VPN tunnel for accessing core network services from home.

Acceptable Use of the Internet in School

1. All students, parents, staff, volunteers and governors are expected to read and follow the acceptable use of the School’s ICT systems and the Internet for adults and students. Visitors will be expected to read and agree to the school’s terms on acceptable use if relevant.
2. 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.
3. Any digital communication between staff and other parties (e.g students, parents/carers) must be professional in tone and content. These communications may only take place on official (monitored) School systems. Personal mobile phones, email addresses, text messaging or social media must not be used for these communications.
4. Personal information should not be posted on the school website and only official email addresses (e.g. pastoral@, studentissues@) should be provided as a point of contact. A means of contacting the School can be found on the 'Contact' page of the School website.
5. We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.
6. More information is set out in the acceptable use agreements in appendices A and B.

Students Using Mobile Devices in School (BYOD)

1. Mobile technology devices may be School owned or personally owned and might include: smartphone, tablet, laptop or other technology that usually has the capability of utilising the school’s wireless network.
2. The device then has access to the wider Internet which may include the school’s websites and other cloud based services such as email and data storage.
3. All users should understand that the primary purpose of the use mobile devices in a school context is educational.
4. Any use of mobile devices in school by students must be in line with the Student BYOD policy.
5. Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.
6. Users must immediately report, to a member of staff, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Staff Using Work Devices Outside School

1. 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, shown in appendix B
2. 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.
3. Any portable storage device containing data relating to the school must be encrypted
4. Not sharing the device among family or friends
5. Work devices must be used solely for work activities
6. If staff have any concerns over the security of their device, they must seek advice from the Network manager

Social Media

1. The School does not currently maintain an official presence on any form of social media.

Protecting Professional Identity - Personal Use by Staff

1. Personal communications are those made *via* a personal social media accounts. In all cases, where a personal account is used which associates itself with the School or impacts on the School, it must be made clear that the member of staff is not communicating on behalf of the School with an appropriate disclaimer. Such personal communications are within the scope of this policy.
2. Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
3. Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
4. When on-site, the School permits colleagues reasonable and appropriate access to private social media sites, outside of directed time.
5. School staff should ensure that:
    1. They do not encourage students to search for their Social Media accounts online.
    2. They do not engage in online discussion on personal matters relating to members of the school community.
    3. Personal opinions are not attributed to the school.
    4. No reference should be made in social media to students, parents/carers or School staff.
    5. It is strongly recommended that security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Educating Students about Online Safety

1. Students will be taught about online safety as part of the curriculum.
2. In Key Stage 3, students 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.
3. Students in Key Stage 4 and 5 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.
4. The safe use of social media and the Internet will also be covered in other subjects where relevant.
5. The school will use assemblies to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

Educating Parents About Online Safety

1. The school will raise parents' awareness of Internet Safety in letters or other communications home, and in information *via* our website. This policy will also be shared with parents.
2. Online safety will also be covered during an annual parents' information evening.
3. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the DSL.
4. Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

Cyber-Bullying

Definition

1. 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.

Preventing and addressing cyber-bullying

1. To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
2. The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes, and the issue will be addressed in assemblies.
3. 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.
4. All staff receive training on cyber-bullying, its impact and ways to support students, as part of ongoing safeguarding training.
5. The school also runs an annual eSafety information evening so that parents are aware of the signs of cyber-bullying, how to report it and how they can support children who may be affected.
6. 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 students, the school will use all reasonable endeavours to ensure the incident is contained.

7. 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.

Examining electronic devices

1. 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 students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.
2. 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:
    1. Cause harm, and/or
    2. Disrupt teaching, and/or
    3. Break any of the school rules
3. 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:
    1. Delete that material, or
    2. Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
    3. Report it to the police.
4. Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.
5. Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school Complaints Policy.

How the School will Respond to Issues of Misuse

1. Where a student misuses the school's ICT systems or Internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.
2. Where a staff member misuses the school's ICT systems or the Internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
3. The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Dealing with potentially criminal issues

1. In the event of suspicion, all steps in this procedure should be followed:
2. Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
3. Conduct the investigation using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
4. It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
5. Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the

content on the machine being used for investigation. These may be printed, signed and attached to the report (except in the case of images of child sexual abuse – *see below*).

6. Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    1. Internal response or discipline procedures.
    2. Police involvement and/or action.
7. If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    1. incidents of grooming behaviour.
    2. the sending of obscene materials to a child.
    3. adult material which potentially breaches the Obscene Publications Act.
    4. criminally racist material.
    5. promotion of terrorism or extremism.
    6. other criminal conduct, activity or materials.
8. Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.
9. It is important that all of the above steps are taken as they will provide an evidence trail for the School and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes.
10. The completed report should be retained by the School for evidence and reference purposes.

Training

1. 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.
2. 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 and staff meetings).
3. 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.
4. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
5. Volunteers will receive appropriate training and updates, if applicable.
6. More information about safeguarding training is set out in our Safeguarding policy.

Monitoring Arrangements

1. The DSL logs behaviour and safeguarding issues related to online safety.

APPENDIX A: Student Acceptable Use Agreement

1. When I use the school's ICT systems (like computers, laptops or accessing school WiFi on my own device) and get onto the Internet in school I will:
    1. Always use the school's ICT systems and the internet responsibly and for educational purposes only
    2. Only use them when a teacher is present, or with a teacher's permission

3. Keep my username and passwords safe and not share these with others
4. 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
5. Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
6. Always log off or shut down a computer when I'm finished working on it

2. I will not
    1. 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
    2. Open any attachments in emails, or follow any links in emails, without first checking with a teacher
    3. Use any inappropriate language when communicating online, including in emails
    4. Log in to the school's network using someone else's details
    5. Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
3. If I bring a personal mobile phone or other personal electronic device into school:
    1. I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
    2. I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online
4. I understand that I am strongly discouraged from arranging to meet anyone offline without first consulting my parent/carer, or without adult supervision.
5. I agree that the school will monitor the websites I visit and understand that there will be consequences if I don't follow these rules

APPENDIX B: Adult Acceptable Use Agreement

1. When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not:
    1. 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)
    2. Use them in any way which could harm the school's reputation
    3. Access social networking sites or chat rooms
    4. Use any improper language when communicating online, including in emails or other messaging services
    5. Install any unauthorised software or connect unauthorised hardware or devices to the school's network
    6. Share my password with others or log in to the school's network using someone else's details
    7. Share confidential information about the school, its pupils or staff, or other members of the community
    8. Access, modify or share data I'm not authorised to access, modify or share
    9. Promote private businesses, unless that business is directly related to the school
2. 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.
3. I agree that the school will monitor the websites I visit.
4. 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.

5. I will let the designated safeguarding lead (DSL) and Network manager know if a student 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.
6. I will always use the school's ICT systems and internet responsibly, and ensure that students in my care do so too.

APPENDIX C: ICT Security for Staff

1. This appendix sets out the required security protocols that all staff using electronic equipment to access School ICT services are expected to follow at all times. The School's electronic systems facilitate detailed access to potentially sensitive student (and staff) data, which we have a responsibility to protect appropriately.
2. No member of staff shall alter settings on School-owned devices to circumvent any of the measures outlined in the policy.
3. Violations of this policy will be handled in line with the School's disciplinary policy.

Multi-Factor Authentication

1. Where available, staff should aim to operate passwordless-ly wherever possible, by using MFA options to access their computer equipment and online services.
2. E.g. Use of a biometric fingerprint to unlock a laptop, the MS Authenticator App to access online services or a plug-in 'YubiKey'.

Password Security

1. Staff passwords are to consist of a minimum of eight characters, and must contain at least one capital letter and a number.
2. Passwords for staff are to be changed three times a year, where practicable.

Mobile Devices

1. Teaching staff are to be supplied with a laptop and charger at the commencement of employment. All ICT equipment will be signed for in the IT support office, against serial numbers, at the point of issue.
2. When a colleague leaves the employment of the School, the equipment is to be returned to the network office, and signed back in. Release of the final month's salary will be contingent on return of the signed-for equipment in acceptable condition; the School reserves the right to make deductions from salary in respect of missing, incomplete or damaged equipment.
3. All School mobile devices will be configured to lock automatically after 30 minutes, before requiring a password to restore access after this time.
4. Before leaving a laptop or mobile device in a room, machines are to be password-locked. Shortcut key: Windows key + L
5. The School reserves the right to reduce the lock period where colleagues fail to adhere to this policy.
6. Where available, additional mobile devices, such as an iPad, are an optional piece of equipment, and are issued on a guarantee basis. In the event of loss or damage due to staff negligence, the School reserves the right to charge the responsible individual the cost of the insurance excess (currently £200).

7. By accepting a School-issue mobile device, users agree to adhere to the following security conditions:
    1. A passcode lock will be enabled with a maximum auto-lock time delay of 5 minutes.
    2. In the case of an iPad, the "Find my iPad" feature must be enabled, and be signed-in with the School's Apple ID, to allow recovery or locking in the event of loss.

School Data

1. With the exception of School email and Teams services for mobile devices (e.g. School email, calendar), staff may not transfer school data onto personally owned computer equipment, or share school data with third parties. Where personally owned equipment is used for BYOD access, security measures (e.g. PIN code, biometric, etc) must be used.
2. Colleagues are strongly discouraged from storing personal data on school-owned devices.
3. Portable storage devices should not be used for transporting sensitive data, due to the risk of loss or theft.
4. Each user account has an associated H: drive which can only be accessed by the owner(s) of the account and network administrators.
5. The open drive (G:) is visible to both staff and student users. Only staff members may modify items on this drive.
6. Files and folders on the iMedia (I:), Staff (U:) and Admin Staff (W:) drives are accessible only to those staff members whose roles require it.
7. New colleagues have a 500Mb Mailbox limit for storing email.
8. In line with the Data Protection Act 2018, colleagues should avoid retaining emails for excessively long periods and should avoid the use of email for expressing personal opinions regarding students or colleagues. Further information can be found in the School's Data Protection Policy.
9. Guidance for colleagues on managing email inboxes can be found on the relevant page of the Staff Handbook.

Staff BYOD

1. For those who choose to connect privately-owned devices to the School's ICT infrastructure, the owner is responsible for ensuring that the device is password-protected when not in use.
2. The School takes no responsibility for the security, safety, theft, insurance and ownership of any device used within the School premises that is not the property of the School. We will investigate the theft not the loss. If a device is stolen or damaged while on School premises, it is to be reported to reception immediately, in order that the incident can be logged.
3. All internet access *via* the School WiFi network is logged.
4. The School does not approve any apps or updates that may be downloaded onto any device whilst using the School's wireless network and such activity is undertaken at the owner's risk, with the School having no liability for any consequent loss of data or damage to the individual's device.
5. Privately-owned devices should not be used in a manner that would portray the School in an unfavourable light while connected to the School's WiFi.
6. Any costs/fees incurred while using devices are not chargeable against the School and are the sole responsibility of the owner.
7. Charging devices of any kind may not be used in School.