Online Safety Policy

Policy Review

This policy has been reviewed by the Digital Safeguarding Lead in conjunction with the DSL.

Review date: Autumn 2025

Contents

1. Aims

We are committed to ensuring the online safety of students, staff, volunteers and governors. We aim to use training, education and effective procedures to both educate and protect the whole school community when they are online. We recognise that the use of technology has become a significant component of many safeguarding issues, including child-on-child abuse. We take any concerns seriously and escalate these where appropriate.

Our school aims to:
- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers and enables 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

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. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationship 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 students' electronic devices where they believe there is a 'good reason' to do so.

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

3. Roles and responsibilities

3.1 The governing board

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

The governor board are responsible for ensuring that the filtering and monitoring system is effective and in place, and regularly reviewed.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is **Karen Powell**

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)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and students with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Headteacher

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

3.3 The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL/ DDSLs) are set out in our child protection and safeguarding policy as well as relevant job descriptions.

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

- In ensuring that staff understand this policy and that it is being implemented consistently throughout the school and understanding the filtering and monitoring systems in place, managing them effectively and how to escalate concerns
- Working with the Digital Safeguarding Lead and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged on CPOMs and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged on CPOMs and dealt with appropriately in line with the school behaviour policy
- 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 governing board

  This list is not intended to be exhaustive.

Our **Designated Safeguarding Leads**
Sarah Holt (DSL)
Ali Newcombe
Maria Krac (DDSLs)
Our **Digital Safeguarding Lead**
Hayleigh Eglinton - Deputy Headteacher

3.4 The ICT provider - BAYTec Technical services

The ICT provider is responsible for:

• Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
• Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
• Conducting a full security check and monitoring the school's ICT systems through a live view system
• Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files in conjunction SWGFL and Smoothwall

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 students 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
• Updating parents around what their children are being asked to do online
• Ensuring that any incidents of cyber-bullying are logged on CPOMs and dealt with appropriately in line with the school behaviour policy
• Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

• Notify a member of staff or the headteacher of any concerns or queries regarding this policy
• Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- National Online Safety (NOS) - app available to all parents / carers
- What are the issues? UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

This list is not intended to be exhaustive.

3.7 Visitors and members of the community

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

4. Educating students about online safety

Students will be taught about online safety as part of our curriculum

In **Key Stage 3**, students 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

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

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns
- By the **end of secondary school**, students will know:
- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships and sex education and health education in secondary schools

The safe use of social media and the internet will also be covered in other subjects where relevant. Our teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and students with SEND.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be available to parents.

Online safety will also be covered during parent events and a drop in session is available for parents on request

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the DSL / DDSLs or Digital Safeguarding Lead

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

6. Cyber-bullying

6.1 Definition

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

6.2 Preventing and addressing cyber-bullying

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.

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. Tutors and Teaching staff are encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected. The school is a member of National Online Safety (NOS) and all parents have access to its resources.

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.

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.

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 students' 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, the staff member must immediately inform the DSL or other member of the senior leadership team who will decide whether they should:
- Delete the material, or
- Retain it as evidence (of a possible criminal offence* or a breach of school discipline), and/or
- Report it to the police**

* If a staff member **believes** a device **may** contain a nude or semi-nude image or an image that it's a criminal offence to possess, they will not view the image but will report this to the DSL (or equivalent) 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.

** Staff will also confiscate the device to give to the police, if they have reasonable grounds to suspect that it contains evidence in relation to an offence.

Any searching of students 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

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

7. Acceptable use of the internet in school

All students, 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 and 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.

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) through Smoothwall to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Students using mobile devices in school

Students may bring mobile devices into school and they must leave them with the Hub on arrival, they are not permitted to use them during:

- Lessons
- Tutor group time
- Clubs or any other activities organised by the school

Any use of mobile devices in school by students must be in line with the acceptable use agreement (see appendix 1).

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.

9. 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 their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

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 IT support or **https://bgcflorguk.sharepoint.com/sites/ITTickets**

10.   How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on ICT systems and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures / staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, ebulletins 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 students can recognise dangers and risks in online activity and can weigh up the risks
- develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL / DDSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

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

12. Monitoring arrangements

This policy will be reviewed every year by the Digital Safeguarding Lead in conjunction with 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 students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff Code of Conduct
- Data protection policy and privacy notices
- Complaints procedure
- ICT systems and acceptable user agreements

Appendix 1: Acceptable use agreement – students and parents / carers

ACCEPTABLE USE OF THE SCHOOL ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS

Name of student:

I will read and follow the rules in the acceptable use agreement policy to keep myself safe

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 only for school purposes

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

I will not:

Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity

- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

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

I will leave it at **the Hub** and I will not take it or use it during lessons, clubs or other activities organised by the school, without an adults permission

- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

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

Signed (Student):	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 students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

I understand that the school will take every reasonable precaution including monitoring and filtering systems to ensure that young people will be safe when they use the internet and ICT systems. I also understand the the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my child's activity on the ICT systems at school will be monitored and that the school will contact me if they have any concerns about any possible breaches of the Acceptable Use Agreement.

I will encourage my child to adopt safer use if the internet and digital technologies at home and will inform the school if I have concerns over heir on line safety.

Signed (parent/carer):	Date:

Appendix 2: Acceptable use agreement – staff

ACCEPTABLE USE OF THE SCHOOL ICT SYSTEMS AND INTERNET AGREEMENT FOR STAFF

Name:

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 students without checking for relevant authorisation to do so
- Share confidential information about the school, its students or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

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

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

I will take all reasonable steps to ensure that work devices are secure and passwordprotected 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 Leads (DSL / DDSLs) and IT Lead 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.

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

Signed:	**Date:**

Appendix 3: Online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident