



**BRIDGEWATER**

HIGH SCHOOL

LEARNING WITH PRIDE AND JOY

# POLICY

## ONLINE SAFETY 2024

Version Number: A24

Ratified by Local Governing Body: [to be ratified]

Next Review Date: March 2025

Prepared by: T Eden



# BRIDGEWATER HIGH SCHOOL ONLINE SAFETY POLICY

<b>Table of Contents</b> .....	Error! Bookmark not defined.
<b>Development/Monitoring/Review of this Policy</b> .....	<b>3</b>
<b>Schedule for Development / Monitoring / Review</b> .....	<b>3</b>
<b>Scope of the Policy</b> .....	<b>3</b>
<b>Roles and Responsibilities</b> .....	<b>5</b>
<b>Governors (Safeguarding Committee):</b> .....	<b>5</b>
<b>Headteacher/Principal and Senior Leaders:</b> .....	<b>5</b>
<b>Online Safety Coordinators:</b> .....	<b>5</b>
<b>Network Manager / Technical staff:</b> .....	<b>6</b>
<b>Teaching and Support Staff:</b> .....	<b>6</b>
<b>Designated Safeguarding Lead:</b> .....	<b>7</b>
<b>Online Safety Group (TE/NRN/SMC/JMS/TH/SH):</b> .....	<b>7</b>
<b>Students / Pupils:</b> .....	<b>7</b>
<b>Parents / Carers:</b> .....	<b>8</b>
<b>Policy Statements</b> .....	<b>8</b>
<b>Education – Students / Pupils:</b> .....	<b>8</b>
<b>Education – Parents / Carers:</b> .....	<b>9</b>
<b>Education – The Wider Community:</b> .....	<b>9</b>
<b>Education &amp; Training – Staff / Volunteers:</b> .....	<b>10</b>
<b>Training – Governors (Safeguarding Committee):</b> .....	<b>10</b>
<b>Technical – infrastructure / equipment, filtering and monitoring:</b> .....	<b>10</b>
<b>Use of digital and video images:</b> .....	<b>11</b>
<b>Data Protection:</b> .....	<b>12</b>
<b>Communications:</b> .....	<b>13</b>
<b>Social Media – Protecting Professional Identity:</b> .....	<b>15</b>
<b>Remote Learning</b> .....	<b>16</b>
<b>Unsuitable / inappropriate activities:</b> .....	<b>16</b>
<b>Responding to incidents of misuse:</b> .....	<b>18</b>
<b>School Actions &amp; Sanctions:</b> .....	<b>19</b>

# BRIDGEWATER HIGH SCHOOL

## ONLINE SAFETY POLICY

### Development/Monitoring/Review of this Policy

This Online Safety policy has been developed by a working group / committee made up of:

- Headteacher/Principal / Principal / Senior Leaders
- Online Safety Coordinators
- Staff - including Teachers, Support Staff, Technical staff
- Governors

### Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Safeguarding Committee.	<i>To be approved</i>
The implementation of this Online Safety policy will be monitored by the:	<i>Online Safety Group</i>
Monitoring will take place at regular intervals:	<i>Once per term</i>
The Safeguarding Committee will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	<i>Every Safeguarding Committee meeting</i>
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	<i>March 2025</i>

The school will monitor the impact of the policy using:

- Logs of reported incidents e.g. via SENSO e.g. trigger words
- Internal monitoring of data within home areas - performed manually through browsing home areas.
- Logs of esafety incidents on CPOMS
- Surveys / questionnaires of
  - students / pupils
  - parents / carers
  - staff

### Scope of the Policy

Online safety is an omnipresent topic which requires recurrent regulatory review and places a stringent duty of care on us all. This policy supports our school in meeting statutory requirements as per the DfE guidance under KCSiE (2023), Working together to safeguard children (2023) and non-statutory guidance, Teaching online safety in schools (2023). The two platforms SENSO and SOPHOS are our primary tools in terms of keeping children safe.

Effective, timely and robust online safety is fundamental to protecting children and young people in education and it is a significant part of the safeguarding agenda. High quality online safety provision requires constant vigilance and a readiness to act where abuse, exploitation or neglect is suspected. The landscape of safeguarding is constantly evolving, and educational establishments must endeavour to embrace and shape their key priorities in support of this. Education has a vital role to fulfil in protecting children and young people from forms of online abuse whilst demonstrating a concerted obligation to respond with haste and flexibility to concerns as they arise. Above all, all staff must foster dedication

## BRIDGEWATER HIGH SCHOOL ONLINE SAFETY POLICY

to ensuring that they listen to the voices of the vulnerable and act upon what is heard. Safeguarding is everyone's responsibility.

Defining online abuse: *"Online abuse is any type of abuse that happens on the web, whether through social networks, playing online games or using mobile phones"* (NSPCC, 2019).

Hidden harms – types of online abuse may include:

- Cyberbullying
- Emotional abuse
- Grooming
- Sexting
- Sexual abuse
- Sexual exploitation

The types, patterns and different circumstances of significant harm and abuse should be considered within the categories identified for children in the Children Act 1989 / 2004. These are:

- Neglect
- Sexual
- Physical
- Emotional

Technology can facilitate a world of learning and development in addition to help yield a range of opportunities. However, the stark reality is that it can also present a window to potential and actual harm and abuse. It can elicit and support an array of illegal abusive behaviours including, but not limited to:

- harassment
- stalking
- threatening behaviour
- creating or sharing child sexual abuse material
- inciting a child to sexual activity
- sexual exploitation
- grooming
- sexual communication with a child
- causing a child to view images or watch videos of a sexual act.

This policy should be read alongside the relevant policies relating to safeguarding of children and in addition to the associated statutory legislation and guidance.

Safeguarding activity across the United Kingdom (UK) continues to intensify in volume and intricacy with national influences relating to political uncertainty, a rise in poverty, an increase in the ageing population, sustained funding pressures and increased demand for child and adult services.

Furthermore, a commitment to ensuring the provision of an integrated and highly robust safeguarding service for all ages is essential. Effective online safety provision and promotion of the welfare of children and young people rely upon constructive relationships that are conducive to robust multi-agency partnership working. This can only be effective when all staff are knowledgeable, confident and equipped with the skills to deal with processes and procedures when concerns arise relating to online abuse or harm.

# BRIDGEWATER HIGH SCHOOL

## ONLINE SAFETY POLICY

Online safety has a high emphasis on a competent well-established workforce, up to date policies and procedures, robust governance arrangements and collaborative practices. Types of online risk usually fall under one of three categories:

**Contact:** Contact from someone online who may wish to bully or abuse the child. This could also include online grooming, online harassment or activities of a commercial nature, including tracking and harvesting person information.

**Content:** Inappropriate material available to children online including: adverts, spam, sponsorship, personal info, violent or hateful content, pornographic or unwelcome sexual content, biased materials, racist materials, and misleading information or advice.

**Conduct:** The child may be the perpetrator of activities including: illegal downloading, hacking, gambling, financial scams, bullying or harassing another child. They might create and upload inappropriate material or provide misleading information or advice.

### **Roles and Responsibilities**

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

#### **Governors (Safeguarding Committee):**

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Safeguarding Committee receiving regular information about online safety incidents and monitoring reports.

- regular updates from the Online Safety Co-ordinators
- awareness of Online Safety Group meetings
- monitoring of a sample of online safety incident logs
- any changes made to filtering / change control routines
- reporting to other relevant bodies

#### **Headteacher/Principal and Senior Leaders:**

- The Headteacher/Principal have a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Co-ordinators.
- The Headteacher/Principal and all members of the Senior Leadership Team must be aware of the procedures to be followed in the event of any online safety allegation being made against a member of staff.
- The Headteacher/Principal are responsible for ensuring that the Online Safety Coordinators and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Leadership Group will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

#### **Online Safety Coordinators:**

- lead the Online Safety Group
- take day to day responsibility for online safety issues and have a leading role in establishing and reviewing the school online safety policies / documents
- provide CPD training and advice for staff, and signpost support for parents/carers (e.g. through National Online Safety)
- liaise with school technical staff

## BRIDGEWATER HIGH SCHOOL ONLINE SAFETY POLICY

- receive reports of online safety incidents; these will be generated by the network manager and/or relevant staff (including incidents on CPOMS) as incidents arise and become part of an overall risk log
- regularly update the Safeguarding Committee with current issues, review incident logs and filtering / change control logs
- report regularly to Senior Leadership Team
- regularly receive updates from external agencies via esafety bulletins and share these with parents/carers where deemed appropriate
- ensure parents are kept abreast of any new technology/concerns the school becomes aware of (e.g. by the media and/or pupils/parents/carers)
- work alongside senior pastoral staff and DSLs to investigate and discipline regarding incidents of online abuse
- use assemblies and/or tutor time to continue to remind pupils of particular current issues regarding online safety and of our expectations regarding acceptable use here in school

### **Network Manager / Technical staff:**

The Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any MAT Online Safety Guidance that may apply
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated through Senso/Sophos working with IWF (Internet Watch Foundation) and CTIRU Counter-Terrorism Internet Referral Unit) constantly updating and monitoring our libraries
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher/Principal; Online Safety Coordinators for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

### **Teaching and Support Staff:**

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher/Principal; Online Safety Coordinators for investigation / action / sanction
- Esafety incidents must be logged on CPOMS and flagged as such so that the Online Safety Lead is fully informed.
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- students / pupils understand and follow the Online Safety Policy and acceptable use policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices

# BRIDGEWATER HIGH SCHOOL

## ONLINE SAFETY POLICY

- additionally, HoYs, AHoYs and Pastoral Support staff are responsible for intervening as appropriate whenever a pupil violation has been flagged by SENSO. This may involve support from the Safeguarding Officer/DSL dependent on the severity/urgency of the violation (see the section on SENSO below).

### **Designated Safeguarding Lead:**

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying
- any other online issues that may have a safeguarding implication

DSLs undergo training every two years and also attend DSL network meetings once per term.

### **Online Safety Group (TE/NRN/SMC/JMS/TH):**

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body – Safeguarding group.

Members of the Online Safety Group (or other relevant group) will assist the Online Safety Coordinators (or other relevant person, as above) with:

- the production/review/monitoring of the school Online Safety Policy/documents.
- the production/review monitoring of the school filtering policy and requests for filtering changes.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/incident logs
- consulting stakeholders – including parents/carers and the students pupils about the online safety provision
- monitoring all of the above plus ongoing improvements through use of the 360 degree safe self-review tool

### **Students / Pupils:**

- are responsible for using the school digital technology systems in accordance with the Student/Pupil Acceptable Use Agreement
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- respect the feelings and welfare of others, both off and online.
- take responsibility for keeping themselves and others safe online.
- are trained in using online media as a power for good, to enhance digital wellbeing
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

### **Vulnerable Learners:**

Many vulnerable children are also those most at risk online; in addition to the harm that this does, it also reduces their opportunity to flourish within the online environment they may find preferable. Over 2 million children in England are living

in families with complex needs. Many children are living in families with domestic abuse, parental substance abuse and mental health problems.



# BRIDGEWATER HIGH SCHOOL

## ONLINE SAFETY POLICY

Bridgewater High recognises that some learners are more vulnerable due to a range of factors. Those children may be:

- Receiving statutory care or support.
- Known to have experienced specific personal harm.
- With a disability, ill-health or developmental difficulties.
- In households or families with characteristics or locations that indicate higher potential likelihood of current and future harm.
- Vulnerable or of concern by virtue of their identity or nationality.
- At risk in relation to activity or institutions outside the home.
- Caring for others.

Bridgewater High will ensure the effective and safe provision of tailored online safety education.

Bridgewater High will obtain input and advice from specialist staff as deemed necessary.

### **Parents / Carers:**

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through newsletters, letters, website / information about national / local online safety campaigns / literature, and the offer of training courses via National College, funded by the school. Parents and carers will be encouraged to support the school in promoting good online safety practice and also to follow guidelines on the need to:

- Be responsible and accountable when taking photos/using technology at school events
- Be fully briefed if involved with actual activities (e.g. supervision on a school trip), particularly with regard to photos and the use of social media.
- Know who the school DSL is.
- Know how to report online issues.
- Report any incidents or issues they become aware of.
- Be a role model for safe and appropriate behaviour.
- Identify and act upon any changes in children's behaviour that could indicate they are at risk of online harm or abuse.

### **Policy Statements**

#### **Education - Students / Pupils:**

Whilst regulation and technical solutions are very important, their use must be balanced by educating students / pupils to take a responsible approach. The education of students / pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

The online safety curriculum is provided in the following ways:

- Internet safety is delivered in Y7, Y8 and Y9 in ICT lessons (whole term's block of work each time).
- PSHE lessons reiterate matters of esafety in every year group.



# BRIDGEWATER HIGH SCHOOL

## ONLINE SAFETY POLICY

- Students / pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students / pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. This includes making clear the correct use of ICT in accordance with exam board regulations in Y10 and above.
- Students / pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making, both through PSHE and individual subject lessons.
- Students / pupils are helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff act as good role models in their use of digital technologies the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students / pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study, particularly with regard to the age and stage of the students involved.

### **Education – Parents / Carers:**

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- The Digital Wellbeing section of our website
- Letters, newsletters, web site, booklets (e.g. Digital Parenting), emails
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. [www.swgfl.org.uk](http://www.swgfl.org.uk) [www.saferinternet.org.uk/](http://www.saferinternet.org.uk/) <http://www.childnet.com/parents-and-carers>
- The provision of training packages via our funded membership with National Online Safety.

### **Education – The Wider Community:**

The school will provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety.
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community, e.g. youth / sports / voluntary groups. This will include signposting.

# BRIDGEWATER HIGH SCHOOL

## ONLINE SAFETY POLICY

### **Education & Training – Staff / Volunteers:**

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- The Online Safety Coordinators will receive regular updates through attendance at external training events (e.g. from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in meetings / INSET days.
- The Online Safety Coordinators will provide advice/guidance/training to individuals as required.
- The provision of training packages via our membership with National Online Safety (now part of National College).

### **Training – Governors (Safeguarding Committee):**

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety / safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (e.g. SWGfL).
- Participation in school training / information sessions for staff or parents.
- The provision of training packages via our membership with National Online Safety.

### **Technical – infrastructure / equipment, filtering and monitoring:**

The school will be responsible for ensuring that the school infrastructure / 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:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will be provided with a username and secure password by the network manager (or Online Safety Lead) who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The “master / administrator” passwords for the school ICT system, used by the Network Manager (or other person) are also available to the business manager and kept in a secure place.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided differentiated user-level filtering (allowing different filtering levels for different groups of users – staff / pupils – or appropriate to age/stage).
- 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 Agreement.

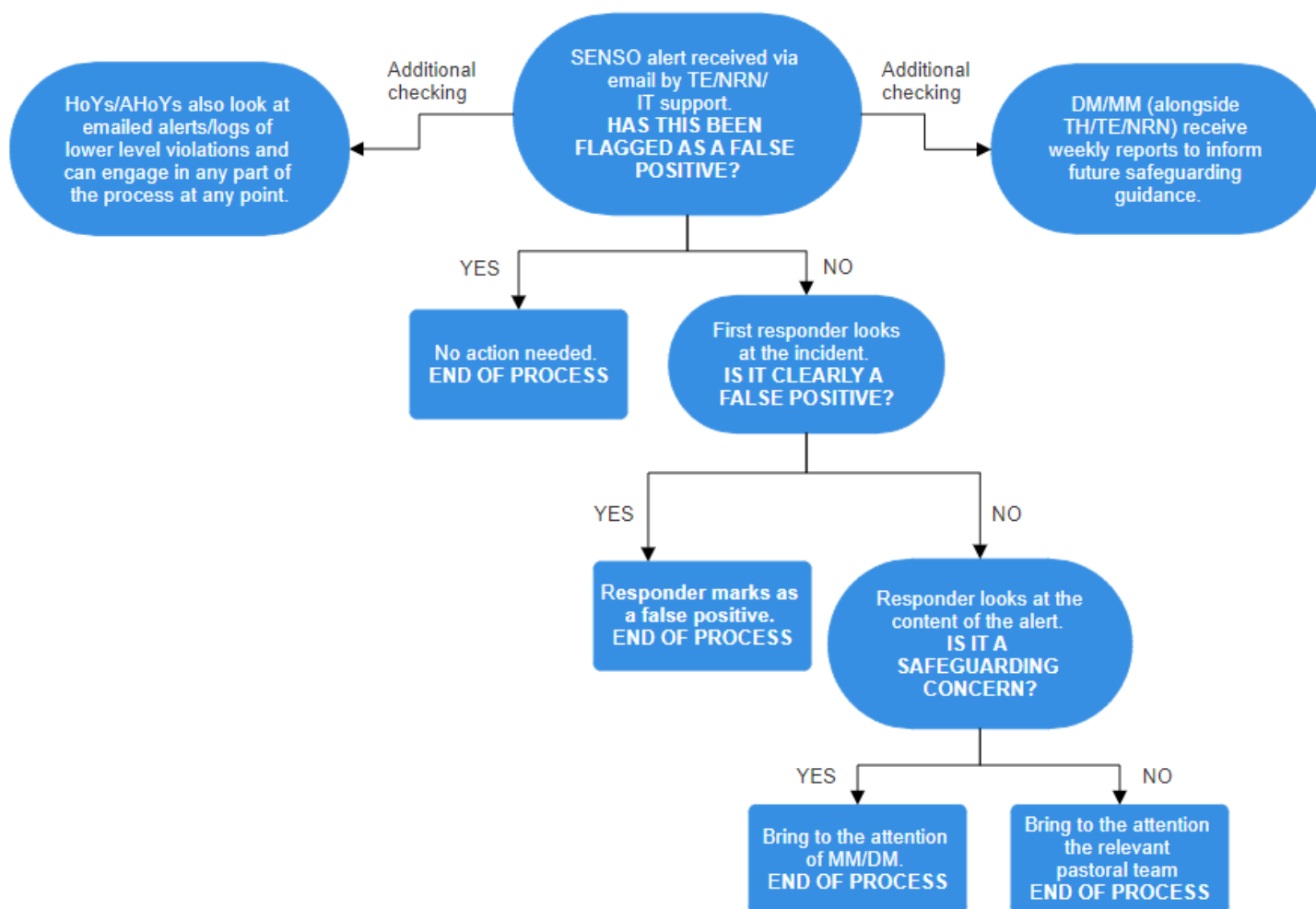
# BRIDGEWATER HIGH SCHOOL ONLINE SAFETY POLICY

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.

## Use of SENSO:

All staff are annually provided with training regarding SENSO and its monitoring capabilities. This is particularly relevant for staff who teach in computer rooms and can use SENSO's further capabilities for monitoring/controlling pupil computers.

The flowchart below shows how the SENSO email alert process is used when violations have been flagged (staff violations are covered separately by SMC, or JMS when SMC is absent).



## Use of digital and video images:

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take

# BRIDGEWATER HIGH SCHOOL

## ONLINE SAFETY POLICY

place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.
- Any new social media site belonging to the school (e.g. Instagram/Twitter feed) has to be signed off in advance by an Assistant Headteacher and Online Safety Coordinator, via a detailed form outlining its use, ownership and governance.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment and only kept on school IT storage systems; they must not be taken home or transferred onto a personal portable/device or emailed to personal email addresses. The personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs, without parental consent.
- Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.
- Where bespoke packages which utilise video images (e.g. Seesaw for assessment of performances) create any additional concerns, parents/carers should be fully informed as to its use and pupils, where appropriate, made to sign individual acceptable use agreements.

### **Data Protection:**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

# BRIDGEWATER HIGH SCHOOL

## ONLINE SAFETY POLICY

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Lock computers even if briefly leaving the room for any reason and if the computer will be unattended for a period of time in an environment where others may view the screen or gain access to data.
- Take care when sharing documents (including photos and videos) either through OneDrive, a Sway, or any other sharing platform that the correct user access has been selected and that no GDPR breaches are taking place e.g. through the use of photographs. Any such breaches should be reported immediately to the Data Protection Officer.

### **Communications:**

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how our permissions for both staff and students.

## BRIDGEWATER HIGH SCHOOL ONLINE SAFETY POLICY

	Staff			Students		
	Allowed	Allowed for certain education purposes	Not allowed	Allowed	Allowed with SLT approval	Not allowed
<b>Communication Technologies</b>						
Mobile phones may be brought to the school						
Use of mobile phones in lessons*						
Use of mobile phones in social time						
Taking photos on mobile phones						
Taking photos on a school camera						
Use of other mobile devices e.g. tablets, gaming devices						
Use of personal email addresses to send emails in school						
Use of school email addresses for non-school use						
Use of messaging apps**						
Use of social media						

\* SLT approves the use of mobile phones according to the following protocols:

- The use of mobile phones must support learning in a clear and recognisable way. This should be planned for and not used ad-hoc or to fill lesson time. In cases where students are specifically given permission, phones should be flat on desks and teachers should circulate their room to ensure that phones are being used only for the intended purpose. The following, for example, would not be considered as an acceptable use: Using to listen to music whilst working.

\*\* Staff should only use messaging apps for brief, urgent staff-to-staff messages (e.g. "Where are we meeting now?") and not for any wider discussion as a group regarding school issues particularly with regard to pupils.



# BRIDGEWATER HIGH SCHOOL

## ONLINE SAFETY POLICY

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students / pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the OSC & DSL – in accordance with the school policy, 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.
- Any digital communication between staff and students / pupils or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students / pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and whilst parents can be instructed as to how to work out a member of staff's email address, these are not to be directly posted on to the school website.

### **Social Media - Protecting Professional Identity:**

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority / academy group liable to the injured party. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through ensuring that personal information is not published.

School staff should ensure that:

- No reference should be made in social media to Bridgewater High School and TCAT students / pupils, parents / carers or school staff (apart from in Bridgewater's own various social media sites)
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- Detailed information regarding who owns/contributes to the sites and for how long

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates



## BRIDGEWATER HIGH SCHOOL ONLINE SAFETY POLICY

itself with the school or impacts on the school/ academy, 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.

- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The school permits reasonable and appropriate access to private social media sites

*See the separate Social Media Policy for further detail.*

### **Remote Learning**

In the case of remote learning (as seen as a result of Coronavirus), teachers must be aware of additional measures which include:

- The use of the waiting lobby is set as standard for each meeting so a teacher must not allow a user to enter if (a) it is an unrecognised name and (b) it has the word Guest underneath it. Such an incident must be passed on to the IT Support team or Online Safety Coordinator.
- The teacher should be the only presenter in a Team (again, set as standard). If a pupil wishes to be unmuted then they can raise their hand for this to be facilitated.
- Pupil cameras should be off at all times (pupils do not have the capacity to unblock this) unless a small group support meeting is taking place facilitated alongside a parent/carer.
- Teachers should be as vigilant as would be expected in a normal classroom with regard to poor behaviour and resolve this through the usual channels (including a screenshot for parents if appropriate).

### **Unsuitable / inappropriate activities:**

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

# BRIDGEWATER HIGH SCHOOL ONLINE SAFETY POLICY

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism					X
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X		
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files						X
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X			
On-line gaming (non-educational)					X	
On-line gambling					X	X*
On-line shopping / commerce				X		
File sharing				X		
Use of social media				X		
Use of messaging apps				X		
Use of video broadcasting e.g. YouTube				X		

\* = student use only

# BRIDGEWATER HIGH SCHOOL

## ONLINE SAFETY POLICY

### **Responding to incidents of misuse:**

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

### **Illegal Incidents:**

In the case of suspected illegal incidents, the information should be passed on to the Headteacher/Principal on the appropriate site who will forward further information to the DSL & OSC. Contact will also be made with the police, parents and any other external body as deemed appropriate, in line with school disciplinary procedures.

### **Other Incidents:**

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- The DSL, OSC and Network Manager are all involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- 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).
- 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 form (except in the case of images of child sexual abuse - see below)
- 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:
  - Internal response or discipline procedures
  - Involvement by external agencies
  - Police involvement and/or action if required
- 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:
  - incidents of ‘grooming’ behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - promotion of terrorism or extremism
  - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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. The completed form should be retained by the group for evidence and reference purposes.

## BRIDGEWATER HIGH SCHOOL ONLINE SAFETY POLICY

### School Actions & Sanctions:

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows

	<b>HANDLED VIA:</b>
Students / Pupils Incidents	
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	DSL & OSC
Unauthorised use of non-educational sites during lessons	Teacher/Line manager
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	Teacher/Line manager
Unauthorised / inappropriate use of social media / messaging apps / personal email	Teacher/Line manager
Unauthorised downloading or uploading of files	Teacher/Line manager
Allowing others to access school network by sharing username and passwords	DSL & OSC
Attempting to access or accessing the school network, using another student's/pupil's account	DSL & OSC
Attempting to access or accessing the school network, using the account of a member of staff	DSL & OSC
Corrupting or destroying the data of other users	Teacher or DSL & OSC
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	DSL & OSC
Continued infringements of the above, following previous warnings or sanctions	DSL & OSC
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	DSL & OSC
Using proxy sites or other means to subvert the school's filtering system	DSL & OSC
Deliberately accessing or trying to access offensive or pornographic material	DSL & OSC
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	DSL & OSC
Staff Incidents	Headteacher/Principal

## BRIDGEWATER HIGH SCHOOL ONLINE SAFETY POLICY

	<b>HANDLED VIA:</b>
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	Headteacher/Principal
Inappropriate personal use of the internet / social media / personal email	DSL & OSC
Unauthorised downloading or uploading of files	DSL & OSC
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	DSL & OSC
Careless use of personal data e.g. holding or transferring data in an insecure manner	DSL & OSC
Deliberate actions to breach data protection or network security rules	Headteacher/Principal
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	Headteacher/Principal
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	Headteacher/Principal
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	Headteacher/Principal
Actions which could compromise the staff member's professional standing	Headteacher/Principal
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	Headteacher/Principal
Using proxy sites or other means to subvert the school's filtering system	Headteacher/Principal
Deliberately accessing or trying to access offensive or pornographic material	Headteacher/Principal
Breaching copyright or licensing regulations	Headteacher/Principal
Continued infringements of the above, following previous warnings or sanctions	Headteacher/Principal

### **THIS POLICY SHOULD BE READ IN CONJUNCTION WITH:**

[Bridgewater Social Media Policy](#)  
[Bridgewater Anti-bullying Policy](#)  
[TCAT Staff Code of Conduct](#)  
[TCAT Disciplinary Policy](#)  
[TCAT Safeguarding and Child Protection Policy](#)