Online Safety Policy

Date Policy Updated:	April, 2026
Leadership team responsibility	Brian Blake, IT Assistant/Health and Safety Lead
To Present to A&P Committee	May, 2026
Date Policy Ratified:	May, 2026
Date for next Review:	October, 2026

Contents

1. Aims 3
2. Legislation and guidance 3
3. Roles and responsibilities 4
3.1 The Governing Body 4
3.2 The Headteacher 4
3.3 The Designated Safeguarding Lead (DSL) 5
3.4 The Network Manager 5
3.5 All staff and volunteers 5
3.6 Parents and Carers 5
4. Educating pupils about online safety 6
Key Stage 3 6
Key Stage 4 6
5. Educating parents and carers about online safety 7
6. Cyber-bullying 8
7. Acceptable use of the internet in school 9
8. Pupils using mobile devices in school 10
9. Staff using work devices outside school 10
10. How the school will respond to issues of misuse 11
11. Training 12
12. Monitoring arrangements 12
13. Links with other policies 13
Appendix 1: Acceptable Use Agreement (Pupils and Parents/Carers) 14
Appendix 2: Acceptable Use Agreement (Staff, Governors, Volunteers and Visitors) 16
Appendix 3: Online Safety Training Needs – self audit for staff 18
Appendix 4: Staged parent notification letters – misuse of internet and digital technologies 19
Letter 1 – Reminder of expectations following an online safety incident 19
Letter 2 – Repeated misuse: parent meeting request 20
Letter 3 – Final letter: further sanctions and referral to external support 21

Vision Statement

Believe Strive Succeed

Our vision is to provide an outstanding, inclusive and aspirational education for local children. We believe that everyone in our community is capable of achieving beyond their expectations by living each day in all its fullness, spiritually, physically, intellectually, emotionally and morally. We are underpinned by deep rooted values of respect, consideration, loyalty, responsibility and success.

1 Corinthians 12:12 'the body is one and has many members, and all the members of the body, though many, are one body'

1. Aims

Bishop Stopford's School aims to:

- Have robust processes in place to ensure the online safety and digital wellbeing of pupils, staff, and the wider school community.
- The school seeks to educate pupils in the safe, responsible and respectful use of digital technologies
- Identify, support and protect pupils who may be at greater risk online
- Maintain clear procedures for reporting, managing and escalating online safety concerns.

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, anti-Semitism, 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 scam

2. Legislation and guidance

This policy reflects statutory guidance and legislation and is based on the Department for Education's (DfE) statutory safeguarding guidance, **Keeping Children Safe in Education (2025)**, and its advice for schools on:

- Keeping Children Safe in Education (2025)
- Teaching online safety in schools

- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships education and, where applicable relationships and sex education (RSE)
- Searching, screening and confiscation

It also refers to the DfE's guidance on **protecting children from radicalisation** and the school's responsibilities under the Prevent Duty.

This policy 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, the Data Protection Act 2018**, **UKGDPR and the Searching, Screening and Confiscation guidance**. In addition, it reflects the **Education Act 2011**, which gives teachers stronger powers to tackle cyber-bullying, including searching for and deleting inappropriate images or files on pupils' electronic devices where there is 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 Body

The Governing Body holds strategic responsibility for online safety and monitoring. The Headteacher is responsible for ensuring the policy is implemented consistently across the school. The Designated Safeguarding Lead (DSL) has lead responsibility for online safety within the wider safeguarding framework.

All staff, volunteers and governors are responsible for implementing this policy and responding appropriately to concerns. Pupils and parents are expected to support the school's approach to online safety.

The Governing Body may also if required coordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

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 some pupils with special educational needs and/or disabilities (SEND).

3.2 The Headteacher

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

3.3 The Designated Safeguarding Lead (DSL)
Details of the school's Designated Safeguarding Lead (DSL) and any deputy DSLs are set out in the Child Protection and Safeguarding Policy.

The DSL has **lead responsibility for online safety within the wider safeguarding framework and is responsible for:**

- Supporting the Headteacher to ensure staff understand this policy and implement it consistently
- Working with the Headteacher, Network Manager and other staff, to address online safety concerns or incidents
- Ensuring that any online safety incidents are recorded and managed appropriately via CPOMS in line with this policy and safeguarding procedures
- Ensuring that incidents of cyber-bullying are recorded and in line with the school's Behaviour Policy
- Coordinating and supporting staff training on online safety supported by the staff training needs audit, appendix 3
- Liaising with external agencies and services where necessary
- Providing regular reports on online safety to the Headteacher and Governing Body

3.4 The Network Manager
The Network Manager is responsible for:

- Implementing and maintaining appropriate **filtering and monitoring systems**, including systems to identify safeguarding risks such as extremist material
- Ensuring the school's ICT systems are secure and protected against viruses and malware,
- Regularly monitoring and reviewing system security and performance
- Blocking access to potentially harmful or inappropriate websites and preventing the downloading of unsafe files where possible
- Supporting the DSL by ensuring relevant technical information is available when online safety incidents arise

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 the policy consistently
- Adhering to the acceptable use of the school's ICT systems and internet (appendix 2), and ensuring pupils follow the pupil acceptable use agreement (appendix 1)
- Reporting online safety concerns promptly and working with the DSL and safeguarding team to ensure incidents are recorded and addressed appropriately
- Responding to incidents of cyber-bullying in line with the school's Behaviour Policy

3.6 Parents and Carers
Parents and Carers are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding online safety
- Ensure their child has read, understood and agreed to the acceptable use of the school's ICT systems and internet (appendix 1)

Parents and carers can seek further guidance on keeping children safe online from:

- UK Safer Internet Centre
- Childnet International
- Disrespect Nobody (Healthy relationships guidance)

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 where relevant and expected to follow it. Where appropriate, they will be required to agree to the acceptable use agreement (appendix 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of a **planned and progressive curriculum**, which is consistent with statutory safeguarding guidance and supports pupils to stay safe online both in and out of school.

All secondary schools are required to teach **Relationships and Sex Education** (RSE) and **Health Education**, which includes aspects of online safety and digital wellbeing.

Key Stage 3

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

- Understand a range of ways to use technology **safely, respectfully, responsibly and securely**, including protecting their online identity and privacy
- Recognise **inappropriate content, contact and conduct**, and understand how and where to report concerns
- Understand the importance of respectful behaviour online, including the impact of online actions on others

Key Stage 4

In **Key Stage 4,** pupils will be taught to:

- Understand how changes in technology affect online safety, including new and emerging risks and ways to protect their privacy and digital identity
- Recognise increased risks associated with online independence, including exploitation, coercion and peer pressure
- Know how to **report a range of online safety concerns** and access appropriate support

By the **end of secondary school**, pupils will know:

- Their **rights, responsibilities and opportunities online**, including that the same expectations of behaviour apply in all contexts, including online
- About a range of **online risks**, including that content shared digitally can be difficult to remove and may be shared beyond its intended audience
- Not to create, share or forward material that they would not want shared further, and not to share personal or sexual content sent to them by others
- What to do and where to get support to **report concerning material or manage online issues**, both within school and externally

- The potential **impact of viewing harmful content** on mental health and wellbeing
- That **sexually explicit material** (for example, pornography) presents a distorted view of relationships and sexual behaviour and can negatively affect attitudes and expectations
- That the **making, sharing or viewing of indecent images of children (including those created by children)** is a criminal offence which carries serious legal consequences
- How information and personal data are **generated, collected, shared and used online**
- How to identify **harmful online behaviours,** including bullying, abuse, harassment, coercion and discrimination, and how to seek help if they are affected

The safe use of social media, online platforms and digital technologies will also be reinforced through other curriculum areas where relevant. Assemblies, form time and curriculum drop-down days will be used to raise awareness of online risks, emerging technologies (including artificial intelligence), and to promote positive digital behaviour. Where appropriate external speakers may be invited support this learning.

5. Educating parents and carers about online safety

The school will raise parents' and carers' awareness of online safety through letters and other communications home, and by providing information via the school website. This Online Safety Policy will also be shared with parents and carers.

Online safety will be addressed where appropriate during parents' evenings and through the safeguarding training calendar across the academic year.

Parents and carers will be contacted following online safety incidents where appropriate, using a staged process aligned with the seriousness and frequency of misuse. Example copies of these communications are included in **Appendix 4**.

The school recognises that parents and carers play a crucial role in supporting children to stay safe online and will encourage a shared, consistent approach between home and school.

If parents or carers have any queries or concerns relating to online safety, these should be raised in the first instance with a member of the safeguarding team

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

The school will make parents and carers aware of

- The **systems and processes** the school uses to filter and monitor online activity on school networks and devices
- The school's expectations of pupils when using digital technologies, both in school and when representing the school online
- How online safety incidents are recorded, monitored and escalated in line with safeguarding procedures
- How parents and carers can access **support, advice and reporting routes** to help keep children safe online
- Where to find further information and guidance to support safe and responsible online behaviour at home

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps, online forums, email or gaming sites. Like other forms of bullying, it may involve repeated behaviour intended to harm an individual and may include an imbalance of power.

The school recognises that **not all harmful online behaviour is repetitive**, and a **single incident** may still constitute bullying or a safeguarding concern, particularly where it involves sexual harassment, threats, coercion, discriminatory language or the sharing of harmful content.

Cyber-bullying is recognised as a form of **child-on-child abuse** and may require a safeguarding response.

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, the school will ensure that pupils understand what it is, the different forms it may take, and what to do if they become aware of it happening to themselves or others. Pupils will be encouraged to report concerns, including where they are a witness rather than the target.

The school will actively discuss cyber-bullying with pupils, explaining why it occurs, the impact it can have, and the potential consequences. Form tutors will address cyber-bullying within tutor groups, and the issue will be reinforced through assemblies. Teaching staff are encouraged to use relevant areas of the curriculum, including **PSHE and RSE**, to explore online behaviour, respectful relationships and the impact of online harm.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its potential impact and how to support pupils, as part of safeguarding training (see section 11)

The school website provides links to trusted sources of information and advice for parents and carers to help them identify signs of cyber-bullying, understand reporting routes and support children who may be affected.

When a cyber-bullying incident occurs, the school will follow the procedures set out in the **Behaviour Policy** and **Child Protection and Safeguarding Policy**. Where illegal, inappropriate or harmful material has been shared, the school will take reasonable steps to limit the spread of the material and support those affected.

The Designated Safeguarding Lead (DSL) will consider whether incidents meet the threshold for a safeguarding concern and whether referral to external agencies, including the police, is necessary.

6.3 Examining electronic devices.

School staff have statutory powers under the **Education and Inspections Act 2006** as extended by the **Education Act 2011** to search for and, where appropriate, delete data or files from pupils' electronic devices where there **is good reason** to do so.
An electronic device includes any device capable of storing digital information, such as mobile phones, tablets, laptops (including Chromebooks), computers, removable storage media and smart devices. This list is not exhaustive.

When considering whether there is a good reason to examine data or files, staff must reasonably suspect that the device has been used, or could be used, to:

- Cause harm to a pupil or others, and/or
- Disrupt learning or undermine the safe environment or the school; and/or
- Facilitate a breach of school rules or the commission of an offence

If inappropriate material is found, the staff member will consult with the DSL or an identified member of the senior leadership team to decide whether to:

- Delete that material, where lawful and appropriate; and/or
- Retain the material as evidence of a breach of school discipline or a suspected criminal offence; and/or
- Refer the matter to the police or other external agencies

Any searching, screening and confiscation will be carried out in accordance with:

- DfE's guidance on **Searching, Screening and Confiscation**
- UKCIS guidance on **Sharing nudes and semi-nudes: advice for education settings working with children and young people**
- The school's behaviour, safeguarding and complaints procedures

Where there is a suspected safeguarding concern, staff will **not view images of an indecent nature**, and the matter will be referred immediately to the DSL, who will decide the appropriate course of action

Any complaints about searching or deletion of data on pupils' electronic devices will be managed through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents and carers, staff, volunteers and governors are expected to read, understand and 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 acceptable use terms where relevant.

The school's internet and digital systems must be used **responsibly, safely and appropriately**. Use of the school's internet and ICT resources must be for **educational purposes** or for the fulfilment of an individual's professional role.

The school operates **filtering and monitoring systems** to help safeguard pupils and staff when using school networks and devices. The use of the school's ICT systems, including access to websites and digital platforms, may be monitored in line with safeguarding obligations. Monitoring is carried out in a **proportionate and lawful manner** to support pupil safety and wellbeing.

Any misuse of the school's ICT systems or internet will be addressed in line with the relevant policies, including the **Behaviour Policy**, **Child Protection and Safeguarding Policy**, and **Staff Code of Conduct**, and may result in sanctions.

Further detail about acceptable use, expectations and responsibilities is set out in the acceptable use agreements contained in **appendices 1 and 2**.

8. Pupils using mobile devices in school

Mobile phones, headphones/earbuds (including AirPods) and other personal electronic devices (for example tablets) **must not be used during the school day** unless permission has been explicitly given by a member of staff. Devices should be switched off by **8:30am** and stored securely in pupils' bags whilst on the school site. Games consoles and similar devices are not permitted in school.
Where a device is seen or used in breach of these expectations, it may be **confiscated** in line with the school's Behaviour Policy. Confiscated devices will be taken to the Headteacher's PA's office and may be collected by the pupil after **48 hours**, before **3:30pm**. Where a device needs to be returned earlier, a parent or carer must attend the school to collect it in person.

The school does not accept responsibility for the **loss, damage or theft** of personal mobile devices brought onto the school site. Pupils are expected to follow instructions relating to mobile devices at all times, and failure to comply may result in further sanctions.

Any permitted use of mobile a device~~s~~ in school must be **in line with the pupil Acceptable Use Agreement** (appendix 1).

A breach of the Acceptable Use Agreement or misuse of a mobile device may result in disciplinary action in accordance with the **Behaviour Policy.** Where misuse raises safeguarding concerns, the matter will be escalated to the **Designated Safeguarding Lead (DSL)** and managed in line with the school's safeguarding procedures.

9. Staff using work devices outside school

Staff members using a school-issued device outside the school site must ensure that it is used **securely and responsibly** and in line with the school's **Acceptable Use Agreement** (appendix 2), the **Data Protection Policy** and the **Staff Code of Conduct**.

Staff must not install unauthorised software or applications on work devices and must not use school devices in any way that would compromise safeguarding, data protection, or the professional standards expected of staff.

Work devices must be:

- Password-protected using secure passwords
- Kept physically secure at all times when in use outside school
- Locked when unattended
- Used only by the authorised member of staff

Any removable media (such as USB devices) containing school data must be **encrypted** and used only where absolutely necessary.

If staff have any concerns regarding the security of a work device, data protection, or potential loss or compromise of data, they must seek advice immediately from the **Network Manager** or the **Designated Safeguarding Lead (DSL),** and follow the school's data protection and incident reporting procedures.

School-issued devices must be used solely for work-related purposes.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems, internet or digital technologies, the school will respond in line with the **Acceptable Use Agreement, Behaviour Policy,** and **Child Protection and Safeguarding Policy**. Actions taken will be **proportionate**, taking into account the nature, context and seriousness of the incident, and the needs of those involved.

Some incidents of online misuse may constitute a **safeguarding concern**, particularly where they involve harm, sexual content, harassment, coercion, discrimination, exploitation or extremist material. In such cases, concerns will be escalated promptly to the **Designated Safeguarding Lead (DSL)** and managed in accordance with safeguarding procedures, including recording incidents via CPOMS.

Where a staff member misuses the school's ICT systems or the internet; or misuses a personal device in a way that constitutes misconduct or breaches professional expectations, the matter will be addressed in accordance with the **Staff Code of Conduct, Acceptable Use Agreement**, and relevant disciplinary procedures. The response will be proportionate and aligned with the seriousness of the incident.

The school will consider whether incidents involve illegal activity or content and, where appropriate, will liaise with external agencies, including the police. The DSL will support decision-making relating to safeguarding thresholds and referrals.

All incidents will be handled sensitively and fairly, with due regard to data protection, confidentiality and the welfare of all members of the school community.

Where appropriate, parents and carers will be informed of incidents involving misuse of the internet or digital technologies. The school uses a **staged approach to parental communication**, which may include:

- An initial letter reminding pupils and parents of expectations following an incident
- A second letter following repeated misuse, requesting a meeting with parents or carers
- A final letter outlining further sanctions and referral to external agencies for additional support, where appropriate

Copies of these letters are provided in **Appendix 4**.

Further operational guidance for staff on managing incidents of inappropriate use of technology, including repeated misuse, behaviour involving personal devices, and incidents

involving AI-generated or manipulated content, is set out in the school's **Guidance on Managing Inappropriate Use of Technology, Online Behaviour and AI-Generated Content**.

11. Training

All new staff members, including temporary, supply and agency staff, will receive **online safety and safeguarding training as part of their induction.** This will include guidance on safe internet use, online safeguarding risks, child-on-child abuse, cyber-bullying and the risks associated with online radicalisation and extremism.

All staff will receive **refresher training at least annually** as part of the whole-school safeguarding training. In addition, staff will receive relevant updates throughout the year, for example through staff briefings, safeguarding bulletins, emails, and staff meetings, to ensure they remain aware of emerging online safety risks and local procedures.

The **Designated Safeguarding Lead (DSL)** and any deputy DSLs will undertake **child protection and safeguarding training**, which will include online safety, at least every **two years**, and will update their knowledge and skills regularly, and **at least annually**, in line with statutory guidance.

Governors will receive **appropriate safeguarding and online safety training**, enabling them to understand their role in online safety oversight, including filtering and monitoring responsibilities.

Volunteers will receive online safety and safeguarding training and updates **as appropriate to their role** and level of contact with pupils.

Further details about safeguarding training and staff responsibilities are set out in the **Child Protection and Safeguarding Policy**.

12. Monitoring arrangements

The school has appropriate monitoring arrangements in place to help ensure a **safe and supportive online environment** for pupils and staff.

Online safety-related safeguarding concerns and behaviours are recorded **via CPOMS** and monitored by the **Designated Safeguarding Lead (DSL)** and safeguarding team. Records of incidents are maintained through **CPOMS**, and relevant actions are planned and reviewed in accordance with safeguarding procedures.

Web filtering and monitoring

Internet access is filtered to help block **inappropriate or harmful content** while allowing legitimate educational use. Monitoring systems are used to identify potential safeguarding concerns, including flagged searches or online activity that may indicate risk. Reports may be generated to support safeguarding investigations where appropriate.

The school uses a combination of filtering and monitoring systems, including **Impero and Senso**, to help identify concerning patterns of online behaviour. These systems support safeguarding by alerting staff to potential risks and do not replace professional judgement.

Digital Platforms
The use of school-approved digital platforms and online services is monitored to help prevent misuse and promote responsible, safe and respectful online behaviour. Monitoring is proportionate and focused on safeguarding and welfare rather than routine surveillance.

Education and Guidance
Monitoring arrangements are supported by ongoing **education and guidance** for pupils and staff. This ensures that online safety is understood as part of a whole-school safeguarding approach and that pupils are encouraged to use technology responsibly.

Incident Reporting and response
Any online safety concerns or incidents identified through monitoring, staff observations or pupil reports are recorded on CPOMS. The DSL and safeguarding team review incidents, assess risk, and determine appropriate next steps, including contact with parents or carers and referral to external agencies where required.

Filtering and monitoring arrangements are reviewed at least annually by the safeguarding team and senior leaders to ensure they remain effective, proportionate and appropriate to risk.

Filtering and monitoring arrangements will be reviewed following any changes to statutory safeguarding guidance, including updates to Keeping Children Safe in Education.

Monitoring systems are used in a **lawful, proportionate and transparent manner**, in line with data protection legislation and statutory guidance.

Monitoring alerts are reviewed in context and do not automatically indicate wrongdoing; professional judgement is applied at all times

This policy will be reviewed every year, by the Deputy Headteacher. At each review, the policy will be shared with the Governing Body to support effective oversight of online safety, including filtering and monitoring arrangements.

13. Links with other policies

This online safety policy should be read in conjunction with the school's other safeguarding, procedural and operational policies, including:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Code of Conduct
- Data protection Policy and Privacy Notices
- Complaints Procedure
- Acceptable Use Policies
- Searching, Screening, and Confiscation Policy

- Guidance on Managing Inappropriate Use of Technology, Online Behaviour and AI-Generated Content
- E-Safety and Digital Systems Procedures (including filtering, monitoring, device management and technical safeguarding controls)

Appendix 1: Acceptable Use Agreement (Pupils and Parents/Carers)

When using the school's ICT systems (like computers, Google Classroom) and get onto the internet in school:

1. I will only use ICT systems in School, including the internet, e-mail, digital video and mobile technologies for School purposes.
2. I will not download or install software on school technologies.
3. I will only log on to the school network, other systems and resources with my own user name and password.
4. I will not use removable media (such as USB drives) unless there is no alternative, and I understand that any removable media must be checked by the Network Team
5. I will not leave a device that I am logged into unattended or unlocked
6. I will follow the schools ICT security system by setting secure passwords, not reveal them and change them regularly.
7. I will disable cellular internet connection whilst in school on any device and connect to the internet only through the school wireless system.
8. I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible.
9. I will be responsible for my behaviour when using the internet. This includes resources I access and the language I use.
10. I will not access or attempt to access accounts belonging to other users.
11. I will not deliberately browse, download, upload or forward material that could be considered inappropriate or illegal. If I accidentally come across any such material, I will report it immediately.
12. Images of pupils and/or staff will only be taken, stored and used for school purposes in line with school policy and not distributed outside the school network without the permission of the Headteacher.
13. I will follow guidance and advice to ensure I use the internet and related digital technologies safely. I will not give out personal information such as name, address or phone number. If I am concerned about mine, or someone else's, safety online I will speak to an adult.
14. I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring into disrepute.
15. I will support the school approach to online safety and not deliberately upload or add any images, video, sounds, or text that could upset any member of the school community.
16. I will respect the privacy and ownership of others work on-line at all times. This includes respecting all copyright laws and never knowingly plagiarising another person's work.
17. I will not attempt to bypass the internet filtering system.
18. I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available to teachers.
19. I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied, and my parent/carer may be contacted.
20. I will tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others and understand that I can contact the ThinkUKnow website to report this material as well.

21. If I am involved in or witness online behaviour that may be harmful, abusive or illegal, I understand this may be treated as a safeguarding concern and shared with the Designated Safeguarding Lead.
22. I will not arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision.
20. I understand that personal mobile phones or other personal electronic devices are not to be used in school unless instructed to do so by a member of staff and that they may be confiscated if seen or being used without permission. https://www.thinkuknow.co.uk/ http://www.ceop.police.uk/Safety-Centre/ To report abuse click on or type in this link.

Appendix 2: Acceptable Use Agreement (Staff, Governors, Volunteers and Visitors)

ICT and related technologies such as e-mail, the Internet and mobile devices are an expected part of our daily working life in school. The policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents.

Any concerns or clarification should be discussed with the Designated Safeguarding Lead Officer. Staff should be aware that a breach of this acceptable use policy may amount to misconduct and result in disciplinary proceedings.

When using the school's ICT systems (like computers, Google Classroom) and get onto the internet in school:

1. I will only use the schools email/Internet/Intranet/learning platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
2. I will limit the use of the internet for personal use to out of lesson time for teaching staff and to breaks and lunchtime for support staff.
3. I will confine my use of my personal mobile phone to private staff areas only.
4. I will comply with the ICT system security and ensure that I keep my password secure and ensure staff pages cannot be accessed by pupils by not leaving an unattended computer logged on and unlocked or let students access it.
5. I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
6. I will not give out my personal details, such as mobile phone number and personal email address, to pupils.
7. I will ensure that any personal data (such as data held on BROMCOM) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely at home.
8. I will not install any hardware or software to school devices without the permission of IT services.
9. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
10. Images of pupils and/or staff will only be taken, stored and used for professional purposes and with the written consent of parent, carer or member of staff. (A list of pupils who cannot be photographed for publicity purposes is held in the School Office).
11. I will not use my own mobile phone to record images of pupils. School cameras are available for recording such images. I will not download images of pupils to my own personal devices.
12. I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
13. I understand that monitoring is undertaken lawfully and proportionately to support safeguarding, in line with data protection legislation.
14. I will support the school approach to e-safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
15. I will respect copyright and intellectual property rights.
16. I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
17. I will support and promote the school's online safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
18. I will not accept any current pupil of any age or any ex-pupil of the school under the age of 18 as a friend, follower, subscriber or similar on any personal social media account, including any form of

on-line gaming. 18. I will only use School sanctioned social media accounts for the communicating of official School business or news.

19. I will inform the designated safeguarding lead (DSL) and where appropriate the Network Manager if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
20. I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.
21. I understand that misuse of school ICT systems or failure to follow this agreement may be treated as a safeguarding concern and dealt with in line with safeguarding procedures as well as disciplinary processes.

Appendix 3: Online Safety Training Needs – self audit for staff

Online Safety Training Needs Audit	
Name of staff member/volunteer:	**Date:**
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	
Are you aware of how to report concerns relating to online safety and misuse of digital technology?	

Appendix 4: Staged parent notification letters – misuse of internet and digital technologies

This appendix contains the standard staged letters used to inform parents and carers following incidents of pupil misuse of the school's ICT systems and internet. The letters reflect a graduated response in line with the Acceptable Use Agreement, Behaviour Policy and safeguarding procedures.

Letter 1 – Reminder of expectations following an online safety incident

Date

Address Line 1
Address Line 2
City
Postcode

Parent Salutation

First Letter – Expectations & Incident Details

I am writing to inform you about a recent incident involving **[Student's Name]** and their use of school technology. During monitoring of our digital platforms, it was noted that **[he / she / they]** accessed website(s) that are not appropriate for their age group / and or entered offensive language into online search engines such as Google.

Details of Accessed Content: [Insert details here]

The school's Pupil Acceptable Use policy sets clear expectations for the use of school technology. Students are to use devices and internet access only for education purposes. Accessing inappropriate material or using offensive language is a breach of this policy which the school takes seriously.

At this stage, our priority is to remind **[Student Name]** of these expectations and help them make better decisions online. We ask that you discuss this matter with your child to reinforce the importance of safe, respectful and educational use of the school technology.

Thank you for your cooperation and support.

Name
Head of Year

Letter 2 – Repeated misuse: parent meeting request

Date

Address Line 1
Address Line 2
City
Postcode

Parent Salutation

Second Letter – Parent Meeting Request

I am following up regarding a repeated incident in which **[Student's Name]** accessed websites that are not appropriate for their age group / and or entered offensive language into online search engines such as Google. Despite our previous letter and discussion with **[Student's Name],** they have again used school technology inappropriately.

Details of Recent Accessed Content: [Insert details here]

This behaviour continues to breach our Pupil Acceptable Use policy and disrupts our efforts to maintain a safe and focused learning environment. At this stage, we need to work closely with you and **[Student Name]** to reinforce clear boundaries and expectations for responsible online behaviour. As such the following sanctions may be put into place

- Restriction of the use of school device privileges for a set period.
- Depending on seriousness of incident possible Early Help referral to be made.
- Risk Assessment to be completed.
- Referral to Inclusion Panel for intervention.

Due to the repeated nature of behaviour, we are requesting a parent meeting to discuss this matter in person. During the meeting we will review our expectations, explore strategies for improvement, and outline the consequences for any further incidents.

Please can you attend school to meet to discuss this concern on _____.

Yours sincerely
Name
Head of Year

Letter 3 – Final letter: further sanctions and referral to external support

Date

Address Line 1
Address Line 2
City
Postcode

Parent Salutation

Final Letter

This letter is to inform you that following multiple incidents of inappropriate technology use, and after our previous discussions on **[insert dates of first and second letters/meetings**], [**Student's Name**] has again accessed websites that are not appropriate for their age group / and or entered offensive language into online search engines.

Details of Most Recent Accessed Content: [Insert details here]

As per our Pupil Acceptable Use policy and school code of the following sanctions may ~~will~~ now be implemented. These include:

- Loss of school device privileges for [insert timeframe]
- Review of risk assessment
- Referral to external agency for additional support.

We encourage you to continue discussing responsible technology use with your child to prevent any further incidents. Please contact me if you have any questions about these sanctions or the next steps.

Yours sincerely
Name
Head of Year