

## Online Safety Policy

BETHANY SCHOOL  
CURTISDEN GREEN  
GOUDHURST  
KENT

<b>Copy Location</b>	<b>Master Copy: Staff Team Policy Channel</b>
----------------------	-----------------------------------------------

<b>Date of Creation</b>	<b>February 2026</b>
<b>Date for Review</b>	<b>September 2027</b>

## Revision History

<b>Version</b>	<b>Date Issued</b>	<b>Reason for Issue</b>
1.0	February 2026	Creation of composite document

## Contents

<b>Scope of the Online Safety Policy.....</b>	<b>6</b>
1.1 Process for monitoring the impact of the Online Safety Policy .....	6
<b>2. Responsibilities.....</b>	<b>6</b>
2.1.1 Headmaster and senior leaders.....	6
2.1.2 Governors .....	7
2.1.3 Designated Safety Lead (DSL) .....	7
2.1.4 Heads of Year / PSHCE Lead .....	8
2.1.5 Teaching and support staff .....	8
2.1.6 IT Provider .....	9
2.1.7 Learners.....	10
2.1.8 Parents and carers .....	10
2.1.9 Community users .....	10
<b>3. Reporting and Responding .....</b>	<b>11</b>
<b>4. Technology .....</b>	<b>14</b>
4.1 Filtering & Monitoring .....	14
4.2 Filtering .....	14
4.3 Monitoring.....	15
<b>5. Appendix.....</b>	<b>16</b>
<b>6. Acceptable Use Agreements - ICT.....</b>	<b>16</b>
6.1 A1 – Acceptable use of IT Agreement For Learners .....	16
6.1.1 Process.....	16
6.1.2 Text of the Pupil AUP .....	16
Learner Acceptable Use Agreement Form.....	16
6.2 A2 – Acceptable use of IT Agreement For Parents .....	19
6.2.1 Process .....	19
6.2.2 Text of the Parent AUP .....	19
6.2.3 AUP – Acceptable Use of IT For Parents & Guardians .....	19
6.3 A3 – Acceptable use of IT Agreement For Staff Users .....	20
6.3.1 Process .....	20
6.3.2 Text of Staff Code of Conduct .....	20
6.4 A4 – Acceptable use of IT Agreement For Visitors .....	23
6.4.1 Process .....	23
6.4.2 Text of the Visitors AUP .....	23
6.5 A5 Reviewing devices/internet sites (responding to incidents of misuse) .....	25



6.5.1	Process.....	25
<b>7.</b>	<b>C1 School Technical Security Policy (including filtering, monitoring and passwords).....</b>	<b>26</b>
7.1	Introduction.....	26
7.2	Responsibilities.....	26
7.3	Policy statements .....	26
7.4	Password and Authentication Policy .....	28
7.4.1	Password Security – Introduction .....	28
7.4.2	Purpose .....	28
7.4.3	Scope.....	28
7.4.4	Strategic Principles .....	28
7.4.5	Password Standards .....	29
7.4.6	Staff and Pupil Authentication Requirements .....	29
7.4.7	Credential Distribution.....	30
7.4.8	Password Changes and Incident Response .....	30
7.4.9	Account Lockout and Monitoring.....	31
7.4.10	Password Recovery and Reset .....	31
7.4.11	Administrative and Service Accounts .....	31
7.4.12	User Responsibilities.....	32
7.4.13	Governance, Review, and Assurance .....	32
7.5	Filtering and Monitoring .....	33
7.5.1	Introduction to Filtering at Bethany School.....	33
7.5.2	Introduction to Monitoring at Bethany School .....	34
7.5.3	Policy Statements.....	35
7.5.4	Filtering and Monitoring Responsibilities .....	36
7.5.5	Changes to Filtering and Monitoring Systems.....	37
7.5.6	Training/Awareness: .....	39
7.5.7	Audit/Monitoring/Reporting/Review.....	40
7.5.8	Further Guidance .....	40
7.6	Process to report actual and potential technical incidents .....	41
<b>8.</b>	<b>C2 School Personal Data Advice and Guidance already covered elsewhere</b>	<b>42</b>
<b>9.</b>	<b>C3 School Online Safety Policy Template: Electronic Devices - Searching Screening and Confiscation already covered elsewhere .....</b>	<b>42</b>
<b>10.</b>	<b>C4 Mobile Technologies Policy (inc. BYOD/BYOT) .....</b>	<b>42</b>
10.1	Introduction to Mobile Technologies .....	42
10.1.1	Potential Benefits of Mobile Technologies .....	42
10.1.2	Considerations.....	42

File name:	Online Safety Policy	Version	1.0
Author	Katja Thornton	Issue date	16/02/2026
Authorised by	Alan Sturrock	Review date	February 2027



<b>11. C4.1 Mobile Phone and Communication Policy .....</b>	<b>45</b>
11.1 Introduction and summary.....	45
11.2 Policy statements .....	46
11.3 The Yondr Pouch and Mobile Phones.....	46
11.4 Beginning of the Day .....	46
11.5 End of the Day .....	47
11.6 Communication between Pupils and Parents .....	47
11.7 Levels Lists .....	47
11.7.1 Levels List Year 7 to 10 pupils.....	47
11.7.1 Levels List Year 11 pupils .....	48
11.7.1 Forgotten Pouch.....	49
11.7.2 Levels List Sixth Form pupils.....	49
11.8 Mobile Hotspots, Virtual Private Networks and Images .....	50
11.9 Teams, the internet, social media and email .....	50
11.10 Communications between pupils and staff .....	50
11.11 Expectations of pupils .....	50
<b>12. C5 Social Media Policy .....</b>	<b>51</b>
12.1 Social Media and Digital Communications by the School.....	51
12.2 Introduction.....	51
12.3 Scope .....	52
12.4 The School uses the following platforms .....	52
12.4.1 Active Social Media and Online Accounts.....	52
12.4.2 Inactive Social Media and Online Accounts.....	52
12.4.3 Active Departmental Accounts .....	53
12.5 Creating New Social Media Accounts.....	53
12.5.1 Monitoring and Response .....	53
12.5.2 Standards of Behaviour .....	53
12.5.3 Legal Considerations.....	54
12.5.4 Handling Abuse or Inappropriate Content .....	54
12.5.5 Tone and Style of Communication .....	54
12.6 Use of Images and Video.....	54
12.7 Monitoring Online References to the School .....	54
12.8 School Website and Digital Platforms .....	54
12.9 Best Practice Guidance.....	55
12.9.1 Managing Personal Social Media.....	55
12.9.2 Managing School Accounts – Do’s .....	55
12.9.3 Managing School Accounts – Don’ts .....	56

---

File name:	Online Safety Policy	Version	1.0
Author	Katja Thornton	Issue date	16/02/2026
Authorised by	Alan Sturrock	Review date	February 2027



<b>13. C6 Policy on the use of Artificial Intelligence in Schools.....</b>	<b>56</b>
13.1 1 Aims and scope.....	56
13.2 1.1 Definitions .....	57
13.3 2 Legislation .....	57
13.4 3 Regulatory principles.....	58
13.5 4 Roles and responsibilities.....	58
13.5.1 4.0 AI Champion.....	58
13.5.2 4.1 Governing board.....	59
13.5.3 4.2 Headteacher .....	59
13.5.4 4.3 Privacy Compliance Officer (DPO) .....	60
13.5.5 4.4 Designated safeguarding lead (DSL) .....	60
13.5.6 4.5 All staff .....	60
13.5.7 4.6 Pupils .....	61
13.6 5 Staff and governors’ use of AI.....	62
13.6.1 5.1 Approved use of AI .....	62
13.6.2 5.2 Process for approval.....	62
13.6.3 5.3 Data protection and privacy.....	62
13.6.4 5.4 Intellectual property .....	63
13.6.5 5.5 Bias .....	63
13.6.6 5.6 Raising concerns.....	63
13.6.7 5.7 Ethical and responsible use.....	64
13.7 6 Educating pupils about AI .....	64
13.8 7 Use of AI by pupils.....	65
13.9 8 Formal assessments .....	66
13.10 9 Staff training.....	66
13.11 10 Referral to our child protection and safeguarding policy .....	66
13.12 11 Breach of this policy .....	67
13.12.1 11.1 By staff .....	67
13.12.2 11.2 By governors.....	67
13.12.3 11.3 By pupils .....	67
13.13 12 Monitoring and transparency .....	68
13.14 12.1.1 AI Appendix 1: Approved uses of AI tools (table) .....	68

---

File name:	Online Safety Policy	Version	1.0
Author	Katja Thornton	Issue date	16/02/2026
Authorised by	Alan Sturrock	Review date	February 2027

## Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Bethany School to safeguard members of our school community online in accordance with statutory guidance and best practice.

**This Online Safety Policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site.**

Bethany School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

### 1.1 Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- *logs of reported incidents*
- *Filtering and monitoring logs*
- *internal monitoring data for network activity*
- *surveys/questionnaires such as the termly Bullying Survey*

## 2. Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

### 2.1.1 Headmaster and senior leaders

- The Headmaster has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The Headmaster and The Safeguarding Committee members are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

- The Headmaster is responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The Headmaster 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.
- The Safeguarding Committee will receive regular updates from the Designated Safeguarding Lead on the misuse of IT as part of the wider Safeguarding Committee termly meetings.
- The Headmaster will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

### 2.1.2 Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. The appointed Governor for Safeguarding will oversee the Online Safety Policy. In this role they will

- have regular meetings with the Designated Safeguarding Lead / Online Safety Lead
- regularly receive (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually.
- reporting to relevant governors group/meeting
- membership of the IT Steering Committee

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

### 2.1.3 Designated Safety Lead (DSL)

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the safeguarding governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out

- attend relevant governing body meetings/groups
- report regularly to Safeguarding Committee
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

### 2.1.4 Heads of Year / PSHCE Lead

Leads will work with the DSL/OSL to develop a planned and coordinated online safety education.

This will be provided through:

- PSHCE
- assemblies and pastoral programmes
- External speakers
- through relevant national initiatives and opportunities e.g. *Safer Internet Day* and *Anti-bullying week*.

### 2.1.5 Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices as referenced in the employment manual, Section L “Staff Online Safety Guidance” and the staff code of conduct Appendix 4, communication with pupils and former pupils as well as social media.
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they follow all relevant guidance and legislation including, for example, [Keeping Children Safe in Education](#) and [UK GDPR regulations](#)
- all digital communications with learners, parents and carers and others should be on a professional level *and only carried out using official school systems and devices (where staff use AI they should only use school-approved AI services for work purposes which have been evaluated to comply with organisational security and oversight requirements)*
- they immediately report any suspected misuse or problem to *the DSL for pupils and the Headmaster if it relates to a member of staff* for investigation/action, in line with the school safeguarding procedures
- online safety issues are embedded in all aspects of the curriculum and other activities

- ensure learners understand and follow the Online Safety Policy and Acceptable Use Policy, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons learners are guided to sites checked as suitable for their use.
- where lessons take place using live-streaming or video-conferencing, there is regard to the requirements of the School Policy.
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.
- they adhere to the school's technical security policy, with regard to the use of devices, systems and passwords and have an understanding of basic cybersecurity
- they have a general understanding of how the learners in their care use digital technologies out of school, in order to be aware of online safety issues that may develop from the use of those technologies
- they are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services, prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated.

### 2.1.6 IT Provider

When using an outside contractor, it is the responsibility of the school to ensure that the provider carries out all the online safety measures that the school's obligations and responsibilities require. It is also important that the provider follows and implements school Online Safety Policy and procedures.

The IT Provider is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack

- the school meets (as a minimum) the required online safety technical requirements as identified by the [DfE Meeting Digital and Technology Standards in Schools & Colleges](#) and guidance from local authority / MAT or other relevant body
- there is clear, safe, and managed control of user access to networks and devices
- 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
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to [\(insert relevant person\)](#) for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person [\(see appendix 'Technical Security Policy template' for good practice\)](#).
- *monitoring systems are implemented and regularly updated as agreed in school policies*

### 2.1.7 Learners

- are responsible for using the school digital technology systems in accordance with the learner Acceptable Use Policy, Online Safety Policy and Mobile Devices Policy.
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology.
- should avoid plagiarism and uphold copyright regulations, taking care when using Artificial Intelligence (AI) services to protect the intellectual property of themselves and others and checking the accuracy of content accessed through AI services.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

### 2.1.8 Parents and carers

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners' Acceptable Use Policy
- providing access to Smoothwall Hub
- seeking their permissions concerning digital images, cloud services etc.
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.
- Completing an agreement relating to Online Safety.

### 2.1.9 Community users

---

File name:	Online Safety Policy	Version	1.0
Author	Katja Thornton	Issue date	16/02/2026
Authorised by	Alan Sturrock	Review date	February 2027

Community users who access school systems/website/learning platform as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems.

### 3. Reporting and Responding

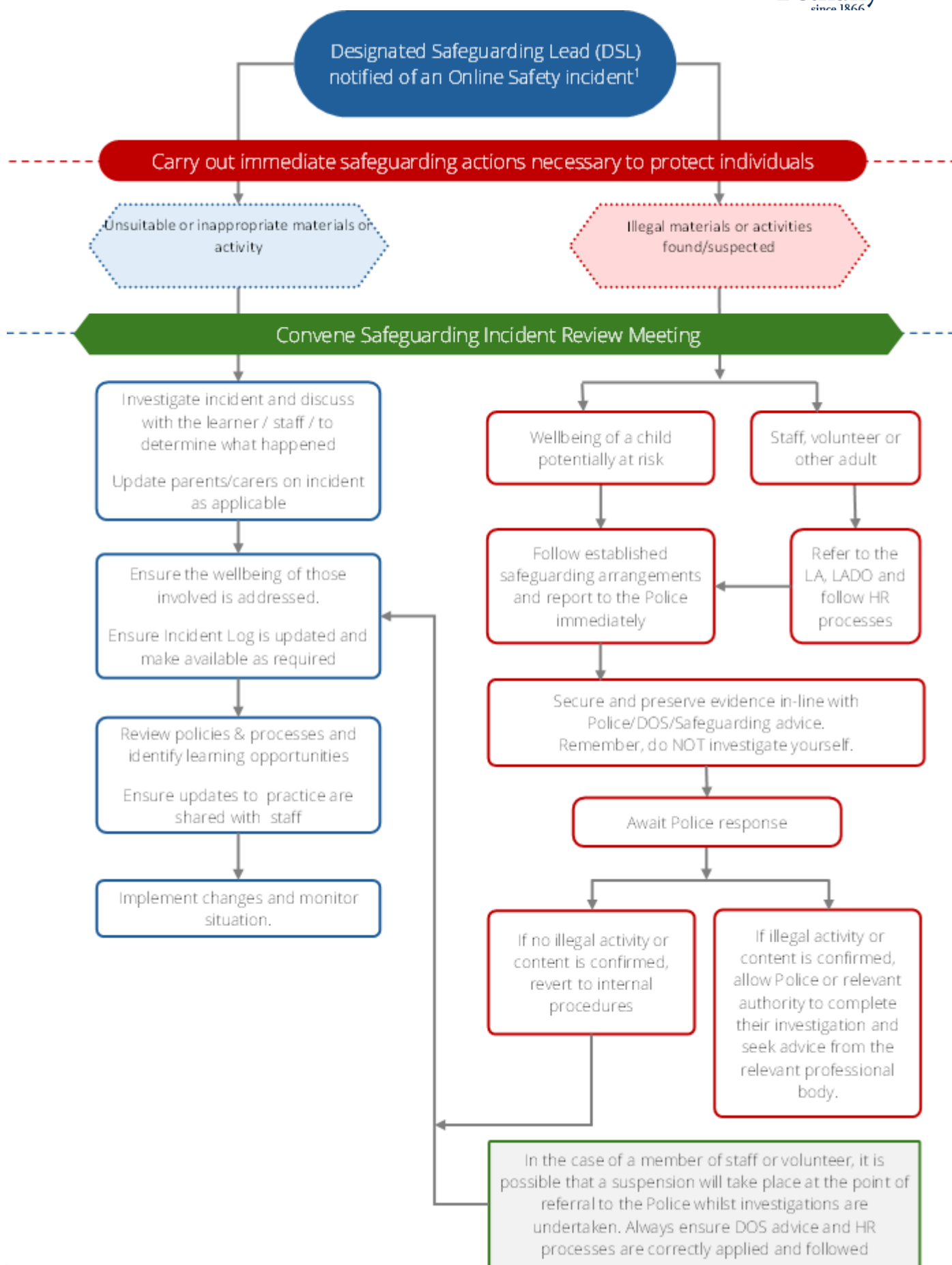
The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing and complaints policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm, the incident must be escalated through the agreed school safeguarding procedures, this may include
  - Non-consensual images
  - Self-generated images
  - Terrorism/extremism
  - Hate crime/ Abuse
  - Fraud and extortion
  - Harassment/stalking
  - Child Sexual Abuse Material (CSAM)
  - Child Sexual Exploitation Grooming
  - Extreme Pornography
  - Sale of illegal materials/substances
  - Cyber or hacking [offences under the Computer Misuse Act](#)
  - Copyright theft or piracy
- any concern about staff misuse will be reported to the Headmaster, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors.
- where AI is used to support monitoring and incident reporting, human oversight is maintained to interpret nuances and context that AI might miss
- where there is no suspected illegal activity, devices may be checked using the following procedures:
  - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
  - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should

illegal activity be subsequently suspected). Use the same device for the duration of the procedure.

- ensure that the relevant staff 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
- 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 local authority / MAT (as relevant)
  - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged by the DSL on the Misuse of IT log.
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police;
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions
- learning from the incident (or pattern of incidents) will be provided to relevant staff

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.



## 4. Technology

The school is 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. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

### 4.1 Filtering & Monitoring

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours. Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility.

The filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.

### 4.2 Filtering

- The DSL and the safeguarding governor are responsible for ensuring these standards are met. Roles and responsibilities of staff and third parties, for example, in-house or third-party IT support are clearly defined.
- the school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE [Filtering standards for schools and colleges](#) and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective. These are acted upon in a timely manner, within clearly established procedures

- there is a clear process in place to deal with, and log, requests/approvals for filtering changes
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- There are regular checks of the effectiveness of the filtering systems . Checks are undertaken across a range of devices at least termly and the results recorded and analysed to inform and improve provision. The DSL and Governor are involved in the process and aware of the findings.
- Devices that are provided by the school have school-based filtering applied irrespective of their location.

### 4.3 Monitoring

The school follows the UK Safer Internet Centre *Appropriate Monitoring* guidance.

**The school has monitoring systems in place, agreed by senior leaders and technical staff, to protect the school, systems and users via Smoothwall Monitoring software.**

- The school monitors all network use across all its devices and services.
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that monitoring is in place.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
- The monitoring provision is reviewed at least once every academic year and updated in response to changes in technology and patterns of online safety incidents and behaviours. The review should be conducted by members of the senior leadership team, the designated safeguarding lead, and technical staff. It will also involve the responsible governor. The results of the review will be recorded and reported as relevant.
- Devices that are provided by the school have school-based monitoring applied irrespective of their location.
- monitoring enables alerts to be matched to users and devices.
- where AI-supported monitoring is used, the purpose and scope of this is clearly communicated

## 5. Appendix

### 6. Acceptable Use Agreements - ICT

#### 6.1 A1 – Acceptable use of IT Agreement For Learners

##### 6.1.1 Process

Pupils are asked to fill in a form on the pupil portal (MSP) when they join and every year in September. Where pupils come from abroad and English language skills are deemed too low to comprehend technical language, a translated copy will be provided to them for signing.

Name or signature and date of submission of the online form are recorded for audit purposes.

##### 6.1.2 Text of the Pupil AUP

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users.

#### Learner Acceptable Use Agreement Form

This agreement is available in other languages.

The School uses an MSP (MySchoolPortal) electronic form for the following agreement, signed by pupils at the beginning of each academic year (or in the first week of starting at Bethany School).

You must agree to use the School's digital systems responsibly to protect your safety, the security of the school systems, and others.

#### PERSONAL SAFETY

The School will monitor my use of its digital systems, devices, and communications (such as Teams and Email). I will not attempt to bypass security systems or use VPNs or hotspots in school.

- I will keep my usernames and passwords secure and private. If compromised, I will report or change them immediately.
- I will only share personal information, like my name or address, when absolutely necessary and with permission.

- I will be cautious when meeting online contacts in person, only doing so with a trusted adult in a public place.
- I will take responsibility for my actions online, using tools like blocking or ending chats if needed.
- I will share images of myself or others only when it is safe and will ensure the images are appropriate and respectful.
- I will only take or share images of myself, or others, when fully dressed. I understand that sharing nude or semi-nude content can cause distress, may be illegal and could lead to prosecution / criminal records.
- I will report harmful or unpleasant material, messages, or anything that worries or upsets me to a trusted adult.
- I will not use school devices or networks for political activity, gambling, personal financial gain, or advertising.

### RESPECTING OTHERS WORK AND INFORMATION

- I will seek permission before using or adapting someone else's work.
- I will verify information I find online, as it may not always be accurate or truthful.
- I will only use Artificial Intelligence (AI) tools approved by the school and ensure my use is ethical, legal, and transparent.
- I will use AI tools only to help me understand or improve my work, not to complete it for me. I will acknowledge any help I receive from such tools.
- I will fact-check and critically evaluate AI-generated content for accuracy, bias, and discrimination before sharing or publishing.
- I will avoid downloading or using copyrighted or protected materials without proper permissions.

### RESPONSIBLE ONLINE BEHAVIOUR

- I will be polite and responsible when I communicate with others. I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions. I will not bully, harass, threaten, upset or make fun of others.

- I will only use platforms or software approved by the school and will not attempt to bypass the filtering/security systems in place. If I become aware of any such attempts, I will report this to a trusted adult.
- I understand cybersecurity poses a risk to both me, other learners and the School and will ensure I take precautions before accessing emails, messages or links. I will check with trusted adults if I have any such concerns.
- I will immediately report any damage, faults or failings involving equipment or software, however this may have happened.
- I understand that misuse of equipment may result in loss of access or other consequences.
- I will follow the age requirements for social media, apps, and tools.
- I will balance my online and offline activities to promote a healthy lifestyle.
- I will protect my online reputation and that of the school, its staff, and other learners.
- I understand that some online behaviours might be regarded, by some, as fun but can have serious consequences – this might include taking (or sharing) images/videos of staff, fights, learners in embarrassing situations or the setting up of fake accounts.
- I will ensure my behaviour reflects positively on the school, both in and out of school settings.
- If required to be learning online from home, I will behave as I would in School. I will be in a suitable space, dressed appropriately, and follow instructions from my teacher.

### CONSEQUENCES OF MISUSE

- I understand that failing to follow this agreement may lead to consequences, including loss of access to the school's systems, detentions, suspensions, contacting parents/guardians, or involvement of the police in serious cases.
- I have read and understand the above and agree to follow these guidelines when:
  - I use the school's systems and devices (both in and out of school)
  - I use my own devices in the school (when allowed)

- I use digital technologies out of the school in a way that is related to me being a member of this School e.g. communicating with other members of the school, accessing school email, website etc.

Name: \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

## 6.2 A2 – Acceptable use of IT Agreement For Parents

### 6.2.1 Process

Parents are asked to fill in and submit the AUP for parents upon joining the school and every year. Name and date of submission are automatically recorded when a parent submits the online form.

### 6.2.2 Text of the Parent AUP

This acceptable use policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and guardians are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The School will try to ensure that learners have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users.

Parents are requested to submit the permission form below to show their support of the School in this important aspect of the School's work.

### 6.2.3 AUP – Acceptable Use of IT For Parents & Guardians

- As the parent/guardian of the above learner, I give permission for my son/daughter to have access to the digital technologies at School.
- I understand that the School has discussed/will discuss the acceptable use agreement with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.
- I understand that the School will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for

---

File name:	Online Safety Policy	Version	1.0
Author	Katja Thornton	Issue date	16/02/2026
Authorised by	Alan Sturrock	Review date	February 2027

the nature and content of materials accessed on the internet and using mobile technologies.

- I understand that my son's/daughter's activity on the systems will be monitored and that the School will contact me if they have concerns about any possible breaches of the acceptable use agreement.
- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the School if I have concerns over my child's online safety.

### CONSENT SUMMARY

#### USE OF CLOUD SYSTEMS

I agree to my child having access to the Microsoft Azure Cloud Services.

#### IMAGE CONSENT REVIEW

I give permission for my child's image to be used - if you choose yes, more options will become available.

Yes/ No

Please tick all that apply:

I give permission for my child's image to be used in printed materials and publicity that Bethany School creates.

I give permission for my child's image to be used on the Bethany School website.

I give permission for my child's image to be used on social media (Facebook, Instagram or X (formerly known as Twitter), Vimeo).

Name: \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

### 6.3 A3 – Acceptable use of IT Agreement For Staff Users

#### 6.3.1 Process

All new members of staff must sign the staff code of conduct/AUP of ICT when they join the School. They are bound by any alterations and additions to the acceptable use agreement while using Bethany School technology.

#### 6.3.2 Text of Staff Code of Conduct

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-safety policy

for further information and clarification. As a new fast developing area of technology, special care and attention must be given to the use of Artificial Intelligence (AI) tools.

**1. I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.**

- I appreciate that ICT includes a wide range of systems, including mobile phones, tablets, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for School business.
  - I understand that school information systems may not be used for private purposes without specific permission from the Headmaster.
  - I will respect system security and I will not disclose any password or security information to anyone other than to the IT Department.
  - I understand that I should not write down or store a password where it is possible that someone may steal it.
  - I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
  - I will not install any software or hardware without permission.
  - I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
  - Where a personal device is used but contains a School application or account, I will use the application separately from personal use.
  - For authorising and verification purposes only, the School may ask me to install an Authenticator app onto my mobile phone or send me a text message, in order to increase security (multi-factor authentication) for certain applications.
  - I will respect copyright and intellectual property rights.
  - I will immediately report any damage or faults involving equipment or software, however this may have happened.
- 2. I understand that it is my duty to promote e-Safety with children in my care, to report any matters of concern, and to use electronic communications of any kind in a professional and responsible manner.**
- I will promote e-safety with children in my care and will help them to develop a responsible attitude to system use, communications and publishing.

- I will report any incidents of concern regarding children's safety to the Deputy Head (Pastoral) a member of the Safeguarding Committee.
  - I will ensure that electronic communications with pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
  - I will communicate with others in a professional manner, I will not use aggressive or inappropriate language, and I appreciate that others may have different opinions.
  - I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so by a member of SMT.
  - I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
  - I will not engage in any on-line activity that may compromise my professional responsibilities.
- 3. I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.**
- The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.
  - I will only use permitted applications to communicate with pupils and will be subject to monitoring purposes to maintain safeguarding standards.
  - I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

I agree to the Terms and Conditions of the Staff Computer Usage Policy

Signed: ..... Print Name: ..... Date: .....

Signature on behalf of the school: ..... Role .....

**6.4 A4 – Acceptable use of IT Agreement For Visitors**

Visitors to the School who need to use Bethany School IT equipment and/ or resources are required to submit the Acceptable use of IT Agreement For Visitors.

6.4.1 Process

- **Ad hoc visitors to the School** sign the AUP statement at Reception when they sign in.
- **Planned visitors** who will bring their own equipment or make extensive use of Bethany School IT systems and networks must complete the [MS365 Visitor Acceptable Use of IT Agreement and IT Needs Form](#) before their visit.
- The member of staff organising the visit is responsible for sending the form to the visitor and confirming on the School Visitors Form that the visitor has been asked to complete it in advance of the scheduled visit.
- Where an electronic submission has not been made for visitors who need extensive access to the school’s infrastructure, a printed copy of the Visitors AUP may be made available.
- Visitors are made aware of the fact that we reserve the right to block access and are encouraged to check accessibility of digital tools and sites.
- We store the form in electronic format within the IT Department Sharepoint site.
- Our entry & exit management system *Inventry* records the submission of the AUP for ad hoc visitors.

6.4.2 Text of the Visitors AUP

We will hold your response to this agreement in electronic format. For further information about our privacy policy and data handling, please check our policy on our website.

<https://bethanyschool.org.uk/school-information/policies/>

Acceptable Use of IT Agreement Statements (MS365 Form)

- I understand that my use of school systems and devices will be monitored.

---

File name:	Online Safety Policy	Version	1.0
Author	Katja Thornton	Issue date	16/02/2026
Authorised by	Alan Sturrock	Review date	February 2027

- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission.
- I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, whatever the cause.
- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this acceptable use agreement, the school has the right to remove my access to school systems/devices.

I have read and understand the above and agree to use the school systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Visitor Name:

Email Address:

Contact name at the School:

Date of proposed visit:

Date of submission:

### 6.5 **A5 Reviewing devices/internet sites (responding to incidents of misuse)**

The following means of recording is used when reviewing devices and/or internet sites when responding to incidents of misuse):

Concerns of misuse can vary significantly in their level of concern they generate. Within the behaviour policy pupils and staff are made aware of a range of responses to the misuse of IT. For low-level concerns these will be recorded within iSAMS as levels. For more significant concerns these will be reported to the Designated Safeguarding Lead who will investigate and record either within the disciplinary structure or the safeguarding structure depending on the appropriate course of action. Misuse of IT is logged by the Designated Safeguarding Lead and is reviewed as part of the termly safeguarding review by the Safeguarding Committee.

#### 6.5.1 Process

Anyone can raise a concern with the IT Department & Deputy Head (pastoral) and request that a device/internet site is reviewed.

The person raising the concern should ask IT staff to carry out the review. IT staff should record the details and conclusions of the concern. A log of submitted investigation details and outcomes is kept by the IT department in the IT department [Reviewing Devices/Internet Sites \(responding to incidents\)](#) Sharepoint list.

## 7. C1 School Technical Security Policy (including filtering, monitoring and passwords)

### 7.1 Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. This is informed by the Department for Education (DfE) guidance, [Keeping Children Safe in Education](#), and the [Digital and Technology Standards](#) and therefore applicable for schools and colleges in England. For schools and colleges outside England, this would be considered good practice, the school should also ensure that they remain compliant with national, local authority or MAT guidance, as relevant. The school is responsible for ensuring that the *school infrastructure/network* is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- access to personal data is securely controlled in line with the school’s personal data policy
- system logs are maintained and reviewed to monitor user activity
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems, including filtering and monitoring provision

### 7.2 Responsibilities

Education settings are directly responsible for ensuring they have the appropriate level of security protection procedures in place in order to safeguard their systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies. The management of technical security is the responsibility of Governors and Senior Leaders, supported in this by the Designated Safeguarding Lead, Online Safety Lead and IT Service Provider.

### 7.3 Policy statements

The school is responsible for ensuring that their 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 receive guidance and training and will be effective in carrying out their responsibilities:

- **school technical systems will be managed in ways that ensure that the school meets recommended technical requirements**
- **cyber security is included in the school risk register.**

- servers, wireless systems, and cabling must be securely located and physical access restricted.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud.
- appropriate security measures (including updates) are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data, including operating systems.
- the school's infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from viruses, worms, trojans etc.
- responsibilities for the management of technical security are clearly assigned to appropriate and well-trained staff at the school
- all users will have clearly defined access rights to school technical systems and accounts are deleted when the user leaves.
- users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- The IT Department, in partnership with Governors/SMT/DSL, regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement. **The School uses Lightspeed filtering and Smoothwall monitoring.**
- Users should report any actual/potential technical incident to the DSL/IT Systems and Data Manager either through the IT Helpdesk or for the DSL through direct email messaging.
- **IT Support Analyst** is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- **guest users are provided with appropriate access to school systems via Bethany Wireless. This does not allow any access to School Sharepoint Sites and is subject to filtering and monitoring either as a pupil or a member of staff depending on their age and requirements.**
- *by default, users do not have administrator access to any school-owned device.*
- an agreed policy is in place regarding the personal use of school owned devices by family members of staff which prohibits all use (Section L of the Staff Employment Manual 2025).

---

File name:	Online Safety Policy	Version	1.0
Author	Katja Thornton	Issue date	16/02/2026
Authorised by	Alan Sturrock	Review date	February 2027

### 7.4 Password and Authentication Policy

(Aligned to UK [NCSC and DfE Guidance](#))

#### 7.4.1 Password Security – Introduction

A safe and secure username/password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and learning platform). The School has a Password Creation and Management Policy in place which follows the standards as set out by the NCSC and DfE.

#### 7.4.2 Purpose

This policy defines how passwords and authentication mechanisms are created, issued, protected, and monitored across the school's systems to:

- Safeguard pupils and staff
- Protect personal and sensitive data
- Reduce the risk of cyber attack
- Support regulatory compliance
- Balance security with accessibility in an educational environment

#### 7.4.3 Scope

This policy applies to:

- All staff, governors, volunteers, contractors, and third-party users
- All pupils issued with school digital accounts
- Administrative, technical, and service accounts
- All school-managed systems, devices, networks, and cloud services

#### 7.4.4 Strategic Principles

The school adopts a risk-based and proportionate approach consistent with national guidance:

- The use of passwords is reduced wherever possible, for example, using Multi-Factor Authentication (MFA) or (Single Sign On) SSO.
- **Passwords when created must be long, unique, and resistant to guessing**
- Routine forced password changes are avoided unless risk requires it
- Higher-risk accounts receive stronger protection

- Multi-Factor Authentication (MFA) is deployed wherever technically possible
- Technical controls supplement user behaviour
- Accessibility and age-appropriate usability are considered for pupils

The school does not publicly disclose internal password-generation methods or security design details.

#### 7.4.5 Password Standards

All user passwords must:

- Meet centrally enforced minimum length requirements
- Avoid predictable patterns or personal information
- Not reuse previous passwords
- Be unique to school systems
- Be protected from automated attack through blocking of common or breached passwords

Complexity rules based solely on character types are not relied upon; strength is achieved primarily through length and unpredictability.

Passwords for standard user accounts do not routinely expire unless compromise is suspected or risk justifies it.

#### 7.4.6 Staff and Pupil Authentication Requirements

##### **Staff and Adult Users**

Staff accounts must:

- Be issued with a temporary password on creation
- Require a password change at first log-in
- Use MFA wherever technically possible, particularly for:
  - Cloud services
  - Remote access
  - Sensitive and protected category data storage and retrieval systems
  - Finance or safeguarding systems
- Have access monitored for suspicious activity

- Be eligible for secure self-service password reset systems

Password managers are encouraged where approved by IT.

### **Pupil Accounts**

Pupil authentication controls are proportionate to age, accessibility, and classroom practicality.

Pupil accounts may:

- Be issued credentials in controlled printed or supervised formats
- Not always be required to reset passwords at first log-in where accessibility or age makes this impractical

In these cases, compensating safeguards must be in place, including:

- Restricted permissions
- Device management
- Web filtering and monitoring
- Login throttling and lockout controls
- Staff- or IT-assisted password reset processes

The school formally records and reviews this risk acceptance annually.

#### 7.4.7 Credential Distribution

Passwords must be issued securely:

- Printed credentials must be sealed and distributed directly to the intended recipient or authorised staff
- Electronic delivery must use approved secure channels
- Passwords must never be sent via open email or informal messaging platforms
- Temporary credentials must expire if unused after a short period

#### 7.4.8 Password Changes and Incident Response

Passwords must be changed immediately where:

- Compromise is suspected or confirmed
- Phishing attempts are reported
- Devices are lost or stolen

- Monitoring indicates abnormal behaviour

Password resets form part of the school's cyber-incident and safeguarding response procedures.

### **Privileged and Administrative Accounts**

Privileged accounts must:

- Be separate from standard user accounts
- Be protected by MFA
- Be subject to enhanced monitoring
- Follow shorter credential rotation where technically required
- Be restricted to authorised personnel only

#### 7.4.9 Account Lockout and Monitoring

Systems must implement:

- Throttling or lockout after repeated failed login attempts
- Alerts to IT for suspicious access
- Logging sufficient for safeguarding investigations and audit
- Detection of anomalous access patterns where supported

Logs are retained in accordance with data-protection and retention policies.

#### 7.4.10 Password Recovery and Reset

Password recovery processes must:

- Verify user identity prior to reset
- Never disclose existing passwords
- Issue temporary credentials that expire quickly
- Require replacement at next log-in
- Use self-service systems only where risk-assessed and approved

#### 7.4.11 Administrative and Service Accounts

Administrative and service accounts must:

- Be documented and assigned an accountable owner

- Be restricted to defined systems and purposes
- Use strong authentication
- Be reviewed regularly

Where possible, password escrow is implemented using an approved encrypted vault or privileged-access management system, with:

- Access logging
- Dual control
- Periodic review

### 7.4.12 User Responsibilities

All users must:

- Keep credentials confidential
- Not share passwords
- Not store passwords insecurely
- Report suspected compromise immediately
- Follow Acceptable Use and safeguarding policies
- Complete cyber-security awareness training when required

Failure to comply may result in restricted access and disciplinary or safeguarding escalation.

### 7.4.13 Governance, Review, and Assurance

This policy is:

- Reviewed annually
- Updated following major incidents or technical change
- Audited internally or externally
- Approved by senior leadership and governors

Compliance is monitored through technical controls, incident reporting, and management review.

## Strategic Improvement Areas

The school will continue to mature controls by:

**Expanding MFA**

Prioritising:

- Staff accounts
- Administrators
- Finance and safeguarding systems
- Remote access services

**Moving Toward Passwordless Authentication**

Assessing:

- Device-based sign-in
- Biometrics
- Security keys for high-risk roles

**Training and Awareness**

Delivering:

- Staff phishing simulations
- Pupil cyber-awareness education
- New-starter briefings

**Approval**

Role	Name / Signature	Date
Chair of Governors		
Headteacher		
Data Protection Officer		

**7.5 Filtering and Monitoring**

**7.5.1 Introduction to Filtering at Bethany School**

Bethany School’s internet filtering system plays an essential role in preventing users from accessing material that is illegal, harmful or inappropriate within an educational environment. Although no filtering system can ever offer a 100% guarantee, due to the dynamic nature of online content and the continual development of new technologies, the school recognises filtering as a core component of a wider approach to online safety, safeguarding, and acceptable use.

---

File name:	Online Safety Policy	Version	1.0
Author	Katja Thornton	Issue date	16/02/2026
Authorised by	Alan Sturrock	Review date	February 2027

**This is a controlled document. If printed it may no longer be valid. The current master version is held in the Staff Team under School Policies**

The school maintains a comprehensive filtering policy to manage associated risks and implement preventative measures appropriate to our setting. In accordance with DfE Keeping Children Safe in Education and the DfE Filtering and Monitoring Standards (2023), we ensure that our filtering provision is appropriate, robust, and aligned with UK Safer Internet Centre definitions.

Our filtering system—provided by Lightspeed—is fully operational, up to date, and applied consistently across:

- all users, including guest accounts
- all school owned devices
- any device accessing the school's wifi connection
- The Lightspeed filtering system is configured to:
  - filter all incoming internet feeds, including backup connections
  - provide age and ability appropriate filtering tailored to educational needs and user group
  - manage multilingual content, images, common misspellings and abbreviations
  - identify and block circumvention attempts such as VPNs, proxies, DNS over HTTPS and similar techniques
  - generates a daily log and is reviewed by the IT Analyst with concerns being reported to the Designated Safeguarding Lead.

The school has verified—through testing via the [SWGfL Test Filtering](#)—that the Lightspeed filtering system prevents access to inappropriate, illegal, or harmful websites, including those identified by national safeguarding bodies. Where users may access content through mobile or app-based technologies, the school seeks confirmation from the provider regarding filtering coverage, and technical monitoring is applied to minimise risk.

Filtering practices are reviewed following any incidents, as well as at least once a year, to ensure ongoing compliance, safety, and effectiveness.

### 7.5.2 Introduction to Monitoring at Bethany School

Monitoring pupil user activity on school devices is a vital part of maintaining a safe environment for learners. Unlike filtering—which blocks harmful content—monitoring enables the school to review pupil user behaviour, identify concerns quickly, and respond appropriately. Effective monitoring relies on timely alerts or observations so safeguarding actions can be taken and recorded without delay.

Monitoring by Smoothwall Monitoring is in place for all school managed laptops used by Years 7–9, providing on site and off site safeguarding oversight.

As the school transitions from a BYOD laptop scheme to a fully managed device model, monitoring coverage may not yet extend to all BYOD devices off site. Coverage will increase as learners move onto school managed laptops.

Monitoring alerts are triaged according to severity:

Level 3, 4, and 5 alerts are sent directly to the DSL for urgent safeguarding response.

Lower level alerts are monitored by the Head of Computer Science, ensuring timely oversight and escalation when needed.

In addition to Smoothwall Monitoring, the School relies on

- o Physical monitoring by staff in classrooms (e.g., Macs in Media, Music and Art)
- o Device management & supervision where appropriate in the boarding houses
- o Individual device monitoring through approved software and third-party systems, such as Classroom Cloud for years 7 &8

DfE Keeping Children Safe in Education requires schools to have “appropriate monitoring,” and the school aligns its practice with the DfE Filtering and Monitoring Standards and UK Safer Internet Centre definitions.

### 7.5.3 Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the School. Illegal content is filtered by the filtering provider (lightspeed) by actively employing the Internet Watch Foundation URL list and other illegal content lists. Filter content lists are regularly updated, and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- There is a filtering and monitoring system in place that safeguards staff and learners by blocking harmful, illegal and inappropriate content.
- There is a monitoring system that enables the prompt investigation of a potential safeguarding incident and outcomes are logged.
- Roles and responsibilities for the management of filtering and monitoring systems have been defined and allocated.
- The filtering and monitoring provision is reviewed at least annually and checked regularly.
- There is a defined and agreed process for making changes to the filtering or monitoring system that involves a senior leader in the agreement of the change.

- Mobile devices that access the school's internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems.
- The school has provided enhanced/differentiated user-level filtering with the Lightspeed filtering system (allowing different filtering levels for different ages/stages and different groups of users – staff/learners etc.).

7.5.4 Filtering and Monitoring Responsibilities

**DfE** Filtering Standards require that schools and colleges identify and assign roles and responsibilities to manage your filtering and monitoring systems, and include

Role	Responsibility	Name / Position
Responsible Governor	Strategic responsibility for filtering and monitoring and need assurance that the standards are being met.	Andrew Cunningham IT & Safeguarding Governor
Senior Leadership	<p>Team Member Responsible for ensuring these standards are met and:</p> <ul style="list-style-type: none"> <li>• procuring filtering and monitoring systems</li> <li>• documenting decisions on what is blocked or allowed and why</li> <li>• reviewing the effectiveness of your provision</li> <li>• overseeing reports</li> </ul> <p>Ensure that all staff:</p> <ul style="list-style-type: none"> <li>• understand their role</li> <li>• are appropriately trained</li> <li>• follow policies, processes and procedures</li> <li>• act on reports and concerns</li> </ul>	<p>Alan Sturrock (DH &amp; DSL) – responsible for decisions around decisions regarding blocking;</p> <p>Francie Healy (Headmaster) responsible for all other decisions around sites that are blocked</p>
Designated Safeguarding Lead	<p>Lead responsibility for safeguarding and online safety, which could include overseeing and acting on:</p> <ul style="list-style-type: none"> <li>• filtering and monitoring reports</li> <li>• safeguarding concerns</li> <li>• checks to filtering and monitoring systems</li> </ul>	Alan Sturrock
IT Service Provider/IT Support	<p>Technical responsibility for:</p> <ul style="list-style-type: none"> <li>• maintaining filtering and monitoring systems</li> </ul>	Zafer Bahriyeli

	<ul style="list-style-type: none"> <li>• providing filtering and monitoring reports</li> <li>• completing actions following concerns or checks to systems</li> </ul>	<p>IT Support Analyst and technical lead</p> <p>Hurst Technologies</p>
<p>All staff</p> <p>need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report if:</p>	<ul style="list-style-type: none"> <li>• they witness or suspect unsuitable material has been accessed</li> <li>• they can access unsuitable material</li> <li>• they are teaching topics which could create unusual activity on the filtering logs</li> <li>• there is failure in the software or abuse of the system</li> <li>• there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks</li> <li>• they notice abbreviations or misspellings that allow access to restricted material</li> </ul>	

### 7.5.5 Changes to Filtering and Monitoring Systems

## Filtering and Monitoring Review and Checks

To understand and evaluate the changing needs and potential risks of the school, the filtering and monitoring provision will be reviewed at least annually. The review will be conducted by members of the senior leadership team, the designated safeguarding lead (DSL), and the IT service provider. Additional checks to filtering and monitoring will be informed by the review process so that governors have assurance that systems are working effectively and meeting safeguarding obligations.

Bethany School’s Filtering and Monitoring Checklist can be found [here](#).

## Reviewing the filtering and monitoring provision

A review of filtering and monitoring will be carried out at least annually to identify the current provision, any gaps, and the specific needs of learners and staff.

The review will take account of:

- the risk profile of learners, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- what the filtering system currently blocks or allows and why
- any outside safeguarding influences, such as county lines
- any relevant safeguarding reports
- the digital resilience of learners
- teaching requirements, for example, the RHSE and PSHE curriculum
- the specific use of chosen technologies, including remaining use of Bring Your Own Device (BYOD)
- what checks are currently taking place and how resulting actions are handled

To make the filtering and monitoring provision effective, the review will inform:

- related safeguarding or technology policies and procedures
- roles and responsibilities
- training of staff
- curriculum and learning opportunities
- procurement decisions
- how often and what is checked
- monitoring strategies

The review will be carried out as a minimum annually, or when:

- a safeguarding risk is identified
- there is a change in working practice, e.g. remote access or BYOD
- new technology is introduced

## Checking the filtering and monitoring systems

Checks to filtering and monitoring systems are completed and recorded as part of the filtering and monitoring review process. How often the checks take place will be based on the context, the risks highlighted in the filtering and monitoring review, and any other risk assessments. Checks will be undertaken from both a safeguarding and IT perspective.

When filtering and monitoring systems are checked this should include further checks to verify that the system setup has not changed or been deactivated. Checks are performed on a range of:

- school owned devices and services, including those used off site
- user groups, for example, teachers, pupils and guests

Logs of checks are kept so they can be reviewed. These record:

- when the checks took place
- who did the check
- what was tested or checked
- resulting actions

The Bethany Filtering and Monitoring Checklist can be accessed via the IT Team SharePoint site [here](#).

### 7.5.6 Training/Awareness:

It is a statutory requirement in England that staff receive training, at least annually, about safeguarding, child protection, online safety and filtering and monitoring. Furthermore, in order to protect personal and sensitive data, governors, senior leaders, staff and learners should receive training about information security and data protection, at least annually.

### Governors, Senior Leaders and staff are made aware of the expectations of them:

- at induction
- at whole-staff/governor training
- through the awareness of policy requirements
- through the acceptable use agreements
- in regular updates throughout the year

Those with specific responsibilities for filtering and monitoring (Responsible Governor, DSL, OSL or other relevant persons) will receive enhanced training to help them understand filtering and monitoring systems and their implementation and review.

### Learners are made aware of the expectations of them:

- in PSHCE and other lessons throughout the curriculum
- through the Learner acceptable use agreements

Parents will be informed of the school's filtering policy through the acceptable use agreement and through online safety awareness information/newsletter etc.

#### 7.5.7 Audit/Monitoring/Reporting/Review

Governors/SLT/DSL/OSL will ensure that full records are kept of:

- Training provided
- User Ids and requests for password changes
- *User logons*
- *Security incidents related to this policy*
- *Annual online safety reviews including filtering and monitoring*
- *Changes to the filtering system*
- *Checks on the filtering and monitoring systems*

#### 7.5.8 Further Guidance

Schools in England (and Wales) are required *"to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering"*. Furthermore, the Department for Education's statutory guidance '[Keeping Children Safe in Education](#)' obliges schools and colleges in England to *"ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness"* and they *"should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system"* however, schools will need to *"be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."* [Ofsted concluded as far back as 2010](#) that "Pupils in the schools that had 'managed' systems had better knowledge and understanding of how to stay safe than those in schools with 'locked down' systems. Pupils were more vulnerable overall when schools used locked down systems because they were not given enough opportunities to learn how to assess and manage risk for themselves."

Bethany School recognises the significant safeguarding risks associated with exposure to terrorist, extremist, and radicalising material online and acknowledges its statutory duty to

mitigate these risks through appropriate filtering and monitoring. At the same time, the school is mindful that overly restrictive or “locked-down” filtering can unintentionally limit learning, inhibit open discussion, and reduce opportunities for pupils to develop the critical thinking skills needed to assess and manage online risk independently. Our approach therefore seeks to strike a careful and proportionate balance: providing robust protection against harmful and illegal content while allowing age-appropriate, supervised access to online resources that support learning, debate, and safeguarding education. Filtering controls are configured to protect pupils without unnecessarily constraining teaching, ensuring that children are supported to explore, question, and understand the world around them in a safe and guided environment.

Where access to legitimate educational content is blocked by Lightspeed Filtering, staff may request a review through IT Services so that learning is not unreasonably restricted. Requests are assessed promptly and proportionately. Where IT staff identify potential safeguarding implications, the decision is escalated to the Designated Safeguarding Lead (DSL) for a decision to release or partially release a website. Where concerns are non-safeguarding in nature—such as disruption risk, gaming functionality, or impact on learning—the matter is referred to the Headteacher for approval. This process ensures that filtering decisions are transparent, risk-based, and aligned with both safeguarding responsibilities and educational priorities.

## 7.6 Process to report actual and potential technical incidents

All IT users should quickly report technical incidents to the IT Helpdesk. IT staff will address system issues promptly and inform staff of relevant risks and solutions as needed.

Staff should report any suspicious link, website, or online content directly to IT without investigating themselves, wherever possible **screenshots** should be taken and sent to the IT helpdesk with a description of the context of what users were trying to access or what they were asked to do.

For device issues, they should contact the IT Helpdesk by email, phone, or in person. This ensures prompt risk management and maintains digital security for all.

When an incident is reported to the IT department and it is suspected that other users may also have been targeted, the IT team will promptly initiate a thorough investigation to determine the scope of the issue. This may involve reviewing access logs to identify if multiple accounts have interacted with a suspicious email or website and scanning the network for signs of malware or unauthorised activity. For example, if a phishing email is reported by one staff member, the IT department will check whether similar messages have been delivered to others and may issue a warning to all users to remain vigilant. In cases where a shared document or network drive is compromised, the IT

team will restrict access, notify potentially affected individuals, and provide guidance on next steps such as password resets or running security scans.

Throughout the process, communication with staff will be clear and timely to ensure that everyone is aware of the risks and the actions being taken to protect the school community.

**8. C2 School Personal Data Advice and Guidance already covered elsewhere**

**9. C3 School Online Safety Policy Template: Electronic Devices - Searching Screening and Confiscation already covered elsewhere**

**10. C4 Mobile Technologies Policy (inc. BYOD/BYOT)**

**10.1 Introduction to Mobile Technologies**

Mobile technologies may be school-owned or privately owned devices, such as smartphones, tablets, or laptops, that can connect to the school's wireless network and access online resources including the learning platform, email, and data storage. Teaching about the safe and appropriate use of mobile technologies must be included in the online safety education programme.

**10.1.1 Potential Benefits of Mobile Technologies**

Research shows that mobile technologies are widely used by both adults and children. Web-based tools have transformed education, granting learners instant access to digital content, databases, and communities. Using these resources effectively, schools can enhance learning and foster digital literacy, fluency, and citizenship, equipping students for a technology-driven world.

**10.1.2 Considerations**

There are a number of issues and risks to consider when implementing mobile technologies, these include; security risks in allowing connections to your school network, filtering of personal devices, breakages and insurance, access to devices for all learners, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership

Schools may consider implementing the use of mobile technologies as a means of reducing expenditure on school provided devices. However, it is important to remember that the increased network management costs and overheads involved in implementing this properly are likely to counterbalance or outweigh any savings.

---

File name:	Online Safety Policy	Version	1.0
Author	Katja Thornton	Issue date	16/02/2026
Authorised by	Alan Sturrock	Review date	February 2027

The use of mobile technologies brings both real benefits and challenges for the whole school community – including teachers - and the only effective way for a school to implement these successfully is to involve the whole school community from the outset. Before the school embarks on this path, the risks and benefits must be clearly identified and shared with all stakeholders.

- The school acceptable use agreements for staff, learners and parents/guardians will give consideration to the use of mobile technologies
- The school allows:

	School/devices			Personal devices		
	School owned and allocated to a single user	School owned for use by multiple users	Authorised device <sup>1</sup>	Learner owned	Staff owned	Visitor owned
Allowed in school	✓	✓	✓	✓	✓	✓
Full network access	✓	✓	✓			
Internet only				✓	✓	✓
No network access						

The school has provided technical solutions for the safe use of mobile technologies in school:

- **Managed school devices are managed through the use of Microsoft’s Mobile Device Management (MDM) software, personally owned devices are monitored where connected to the School’s networks.**
- **Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g Internet only access, network access allowed, shared folder network access)**

---

<sup>1</sup> Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school

- The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices
- For all mobile technologies on the school network, filtering will be applied to the internet connection and attempts to bypass this are not permitted
- Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user. These includes revoking the link between MDM software and the device, removing proxy settings, ensuring no sensitive data is removed from the network, uninstalling school-licensed software etc.
- All mobile devices on the school network are monitored
- The software/apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps
- The school will ensure that devices contain the necessary apps for school work. Apps added by the school will remain the property of the school and will not be accessible to learners on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs.
- Where a school device has been provided to support learning, it is expected that learners will bring devices to the school as required.
- The changing of settings that would stop the device working as it was originally set up and intended to work is not permitted

*When personal devices are permitted:*

- Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/guardians) as does the liability for any loss or damage resulting from the use of the device in school
- The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)
- The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues
- The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security

- The school is not responsible for the day-to-day maintenance or upkeep of the users personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.

Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition:

- Devices are not permitted in tests or exams, except where authorised by the awarding body and under the direction of the Examinations Officer
- there is clear advice and guidance at the point of entry for visitors to acknowledge school requirements by way of signing the conditions of use in the Visitor AUP.
- For BOYD users, they are responsible for keeping their device up to date through software, security and app updates.
- Users are responsible for charging their own devices and for protecting and looking after their devices while in the school
- Confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
- Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
- The expectations for taking/storing/using images/video aligns with the school's acceptable use policy and use of images/video policy. The non-consensual taking/using of images of others is not permitted.
- Devices may be used in lessons in accordance with teacher direction
- Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances

## 11. C4.1 Mobile Phone and Communication Policy

### 11.1 Introduction and summary

The School recognises that there are legitimate reasons for pupils to carry mobile phones, such as for travel arrangements and emergency contact with parents or guardians. However, mobile phones are increasingly becoming a distraction from learning at best, and at worst, are a means of causing harm. Our existing mobile phone policy has been reviewed, and we have found a way to better implement it and enforce existing rules with the simple Yondr pouch scheme.

This policy lays out the rules of mobile phone (and associated accessories) use. Other policies may refer to this policy (Online safety policy) and should be seen as complementary.

## 11.2 Policy statements

Mobile phones are not allowed to be on or used during the school day. Yondr Pouches must be used to store mobile phones and associated accessories during the School day by **all Year 7-10 pupils**. Levels apply where these rules are flouted.

**Year 11 pupils** are currently exempt from the requirement of locking their phone in the Yondr Pouch. However, if a mobile phone is found turned on or being used without the express permission of a member of staff, all Levels described in this policy apply.

**Sixth form pupils** are allowed to use their phone in the Sixth Form centre only. Anyone using their phone outside of this location is also subject to the same Levels described below.

Pupils are expected to check and respond to emails and Teams messages at key times daily, using polite and formal language, and to report any concerning behaviour. Electronic communication after 17:00 on weekdays and during weekends or holidays may not receive a response until the next school day, with exceptions for urgent safeguarding concerns. **All use of school IT systems must remain educational and appropriate, in line with the School's Online Safety and Computer Usage and Behaviour policies.**

## 11.3 The Yondr Pouch and Mobile Phones

Pupils may bring a mobile phone to School for the purpose of safe travel to and from the School. However, mobile phones are not to be used during the School day. Every pupil in Year 7 to 10 is assigned a personal Yondr Pouch. This is a locking Pouch that will prevent access to phones. It is each pupil's responsibility to bring their Pouch with them to school every day and keep it in good working condition. The cost of the pouch is currently £30 including VAT and parents are billed for the initial pouch and any replacement that is necessary due to loss or misuse.

## 11.4 Beginning of the Day

Pupils must bring their Yondr Pouch to School with them each day. As pupils arrive to the School they will:

1. Turn their phone off
2. Open their Yondr Pouch by tapping against the Unlocking Base

3. Place their phone and/or smart watch inside the Yondr Pouch and secure it
4. Store it in their backpack or schoolbag for the day

Staff will be present to oversee and spot-check each morning. If for whatever reason, staff are not present, pupils should still follow this procedure. If pupils have difficulty locking their phone in the Yondr Pouch in the morning, they should report to the School Office or ask any member of staff for help. The absence of staff on a given morning cannot be used to justify having a phone outside of a Yondr Pouch, as the locking works through self-service and support is always available when pupils come to the School Office.

**11.5 End of the Day**

Pupils will visit Unlocking Bases after 16:55 and will:

1. Open their Yondr Pouch
2. Remove their phone and/or smart watch
3. Close their Yondr Pouch (important to stop the pin bending in the bag)
4. Keep in their schoolbag overnight

Late Starters or Early Leavers: Pupils arriving late (after 08:30) or leaving early (before 16:55) will pouch/unpouch their phones in the School Office.

**11.6 Communication between Pupils and Parents**

If pupils need to call home due to an emergency, they may request permission to do so from their Tutor or the Head of Year or Wellness Centre staff. This helps the staff to monitor pastoral concerns. Parents may leave messages with Reception or School Office. Pupils will also be able to pick up messages via email on their laptops and on their phones at 16:55, when pouches are unlocked.

**11.7 Levels Lists**

11.7.1 Levels List Year 7 to 10 pupils

Offence Years 7- 10	Level
---------------------------	-------

---

File name:	Online Safety Policy	Version	1.0
Author	Katja Thornton	Issue date	16/02/2026
Authorised by	Alan Sturrock	Review date	February 2027

**This is a controlled document. If printed it may no longer be valid. The current master version is held in the Staff Team under School Policies**

Phone found outside Yondr during School day unless unlocked by a member of staff for a specific educational purpose	Phone and pouch confiscated for the day and Level 1 issued
Yondr Pouch found to be accidentally unlocked during school day	Phone and pouch confiscated for the day and Level 1 issued
Yondr Pouch found to be deliberately unlocked during school day	Phone and pouch confiscated for the day and Level 2 issued
Repeated offence of above (x2)	Phone confiscated and Level 2 or Level 3 issued as appropriate
Bringing two phones to school to defeat the system	Level 3 issued
Possession of Yondr unlocking station or similar magnet	Level 4 issued
Deliberate damage to or deliberate loss of Yondr Pouch (not reported)	Level 3 issued and replacement cost charged to parents
Accidental damage to or loss of Yondr Pouch (reported)	Repair or replacement cost charged to parents
Phone in Yondr Pouch found to be switched on or goes off	Level 1 issued and pouch & phone confiscated for the day
Coordinated/systematic attempt to damage or defeat Yondr system	Level 4 issued

11.7.1 Levels List Year 11 pupils

Pupils in year 11 are advised to use the Yondr mobile phone pouch during the day but are not obligated to do so. Staff will not be checking pouch use where this is on a voluntary basis.

However, Levels also apply under the following circumstances:

Offence Year 11	Level
-----------------	-------

Phone found switched on and/or outside a schoolbag during school day	Phone confiscated and Level 2 issued
Repeated offence of above	Phone confiscated and Level 3 issued
Repeated for the third time	Mobile Phone Pouch must be purchased and used
Phone goes off	Phone confiscated and level 3 issued
Coordinated/systematic attempt to get around the no phone school policy	Level 4 issued

11.7.1 Forgotten Pouch

If a pupil forgets their Yondr Pouch, they should report to the School Office by 08:30 to hand in their phone. Phones can then be collected at 16:55. If a pupil consistently forgets their Pouch, they will be reported to their Head of Year and their parents will be contacted to discuss next steps.

11.7.2 Levels List Sixth Form pupils

Pupils in Years 12-13 may use their mobile phones in the Sixth Form Centre, or on the direct instruction of a member of staff. They must be switched off during academic lessons, study periods and whilst using the library. A pupil in Years 12-13 who uses their mobile phone outside the 6th form centre will be issued a level and asked to put the mobile phone away.

<b>Offence</b>	<b>Level</b>
<b>Sixth Form</b>	
Phone found outside a schoolbag during school day anywhere on the school site other than the 6 <sup>th</sup> Form Centre.	Phone confiscated for the day and Level 2 issued
Repeated offence of above (x2)	Level 3 issued

Coordinated/systematic attempt to get around the no phone school policy	Level 4 issued
-------------------------------------------------------------------------	----------------

**11.8 Mobile Hotspots, Virtual Private Networks and Images**

Use of “mobile hotspots” or Virtual Private Networks” (VPNs) is not permitted. Any pupil found to be operating a “mobile hotspot” or VPN will receive a Detention after school with their Head of Year. A second offence will lead to a Saturday Detention. Pupils are not permitted to make recordings (images, videos or sound) of pupils or staff without the direct instruction of a member of staff. Recording a pupil or staff member without their consent will lead to a Friday After School Detention.

**11.9 Teams, the internet, social media and email**

Communications in these areas have become very much part of our daily routines.

**11.10 Communications between pupils and staff**

Communications should be appropriate and strictly limited to School accounts. The tone and language of communication should be appropriate. Staff and pupils may ‘chat’ over Teams. Pupil to pupil chat on Teams is not permitted without a member of staff included and should be in relation to school activities.

**11.11 Expectations of pupils**

Pupils are expected to check their emails and Teams messages daily, at the start of the School day, at 13:50 and after school, and respond appropriately. They should not use School systems as an informal means of communication among their peer group, either during the day nor from home. Pupils are asked to report any concerning behaviour or

content to their Tutor or Head of Year. Pupils should use polite and appropriate language in drafting messages; persistent and deliberate inappropriate communication will be escalated as a behavioural matter.

There is an electronic messaging amnesty from 17:00 on weekdays during term time. If a Teams message or email is sent after 17:00, then the sender should not expect a member of staff to see it until the following day. Teachers may still respond in the evening depending on the type of question being asked. Like any query, it may need a very quick response or something more detailed the following day.

Electronic messages received after 17:00 on a Friday during term time week will be responded to by close-of-business the following Monday. Again, the teaching

File name:	Online Safety Policy	Version	1.0
Author	Katja Thornton	Issue date	16/02/2026
Authorised by	Alan Sturrock	Review date	February 2027

staff can exercise their judgement depending on the nature of the query, for instance if it concerns co-curricular activities over the weekend.

Electronic communication in the holidays is at the teacher's discretion. Some communication might be desirable in the run up to trial or other examinations. Therefore, in an academic context, the teaching staff will make every effort to ensure that instructions and resources are clearly set out at the end of a term to limit the need for further communication in the holiday.

Pastoral/safeguarding concerns are exceptions to the time limitations described above, as issues may occur during evenings and weekends. However, it is best for personal or sensitive communication not to remain on Teams or email, where a discussion in person at School would be the most appropriate. If a member of staff is contacted through Teams about a pastoral/safeguarding concern, they will contact the Safeguarding Lead and/or SMT member on duty as soon as possible by contacting the school via email or via the SMT duty phone.

Messaging in Teams should be polite, formal and start with 'Hi or Dear Mrs/Mr and a surname'. Once the communication thread is established, comments do not need to be prefaced with 'Mr/Mrs and a surname'. We believe that these are good communication habits for our pupils to be in.

The School's policy with regard to online behaviour can be found on the Bethany School website/policy section.

Failure to adhere to the protocols outlined in this policy could lead to a disciplinary response under both this policy and the School's 'Behaviour and Discipline Policy'.

It must be remembered that the School's IT services are provided for academic and educational purposes – not for games, socialising and other entertainment. The internet

must not be taken for granted. If accessed material is thought to be illegal, the police may be consulted.

## 12. C5 Social Media Policy

### 12.1 Social Media and Digital Communications by the School

#### 12.2 Introduction

Social media and digital communications are an important part of how Bethany School communicates with its community and the wider public. Social media includes any online platform that enables interaction, sharing of content, or public communication, including video platforms e.g. You Tube.

Bethany School recognises the significant benefits and opportunities that a strong digital and social media presence offers for learning, engagement, marketing and community building. However, the school also recognises the risks associated with online communication, particularly in relation to safeguarding, data protection, cyberbullying and reputation management.

This policy sets out expectations to ensure the safe, responsible and professional use of social media and digital platforms by staff, pupils, parents/carers and the wider school community.

### 12.3 Scope

This policy is subject to the school's Employment Manual, Safeguarding and Child Protection Policy and Acceptable Use Agreements for pupils, staff and parents.

This policy:

- Applies to all staff, contractors and volunteers.
- Applies to all online communications that directly or indirectly represent Bethany School.
- Applies to communications posted at any time and from any location.
- Encourages safe and responsible use of social media through training and education.
- Defines how public social media activity relating to the school is monitored and managed.

Professional communications are those made through official school channels, posted on a school account or using the school's name or branding. These are fully within the scope of this policy. Further guidance is found in staff personal social media in the Employment Manual. This extends also to the Staff Bullying and Harassment Policy.

### 12.4 The School uses the following platforms

#### 12.4.1 Active Social Media and Online Accounts

- Facebook
- Instagram
- LinkedIn
- X
- Vimeo

#### 12.4.2 Inactive Social Media and Online Accounts

- YouTube
- TikTok

#### 12.4.3 Active Departmental Accounts

- Art Department on Instagram (run by Head of Department - Art)
- Food Studies on Instagram (run by Food and Nutrition teacher)
- Business Studies on X (run by Head of Enterprise)

All social media and online accounts, including departmental accounts, are used for the promotion of Bethany School and celebration of pupil achievement by way of text, image and video.

### 12.5 Creating New Social Media Accounts

Any department or group wishing to create a social media account representing Bethany School must submit a proposal to the Head of Marketing outlining:

- Purpose and aims of the account
- Intended audience
- Promotion strategy
- Named staff responsible (minimum of two)
- Whether the account will be public or restricted
- Approval will only be granted once training and understanding of this policy are confirmed.

#### 12.5.1 Monitoring and Response

Official school accounts are monitored regularly by the Marketing Department, ideally daily, including during school holidays. Comments or queries should receive acknowledgement within 24 hours or the next working day by the Marketing team. Monitoring is essential to prevent and address safeguarding concerns, bullying or inappropriate behaviour.

#### 12.5.2 Standards of Behaviour

All digital communications must be professional, respectful and aligned with school values. Users must:

- Maintain confidentiality
- Avoid defamatory or discriminatory content
- Declare identity when posting on behalf of the school

Breaches of this policy may lead to disciplinary action and, where appropriate, referral to external authorities.

### 12.5.3 Legal Considerations

Users must respect copyright and obtain permission before sharing protected content where this is required from the identified holder of the copyright. All use of social media must comply with data protection and confidentiality laws, including UK GDPR.

### 12.5.4 Handling Abuse or Inappropriate Content

Harmful or offensive comments should be addressed promptly and professionally. The school may remove, block or report content and will explain actions taken where appropriate. Abuse must be reported using established safeguarding and reporting procedures – Marketing will report this to the DSL.

### 12.5.5 Tone and Style of Communication

Content published by Bethany School should be:

- Engaging
- Conversational
- Informative
- Professional

## 12.6 Use of Images and Video

Images and videos may only be shared in line with the school's Image and photo consent policy which is sent by the Data Manager via MSP and added to Isams.

Staff must:

- Ensure appropriate permissions are in place
- Respect requests not to be photographed
- Share pupil images only via official channels
- Ensure images are appropriate and respectful
- Delete any potentially compromising images immediately

## 12.7 Monitoring Online References to the School

Bethany School Marketing Team will proactively monitor public online references to protect its reputation and respond appropriately – this is through Google Alerts.

## 12.8 School Website and Digital Platforms

The school website and official digital platforms are extensions of Bethany School's communication strategy and must:

- Present accurate, up-to-date and appropriate information
- Protect personal data and privacy

- Reflect the school's safeguarding commitments
- Follow accessibility and inclusion best practices
- Be managed by authorised staff only

To strengthen the protection of images and personal information published on the school website, Bethany School implements the following technical safeguards where reasonably practicable:

- Disabling right-click image download: Website functionality may restrict right-click options to reduce casual downloading and copying of images.
- Disabling hotlinking: Technical controls are used to prevent external websites from directly embedding or displaying Bethany School images via image URLs.
- Screen capture deterrents: Where possible, protective measures may blur or obscure images when common screen-capture shortcuts are detected. The school recognises that such measures are not completely fail-safe but act as a deterrent.
- Removal of EXIF metadata: Image files published online will have embedded metadata removed where feasible to reduce the risk of identification or long-term tracking of individuals.

Any updates or structural changes to the website must be approved with some oversight of the IT Steering Committee, made up of Governors, Headmaster, Bursar, Deputy Head Academic, Deputy Head Pastoral (DSL), IT Managers and when appropriate the service provider.

## 12.9 Best Practice Guidance

### 12.9.1 Managing Personal Social Media

- Assume nothing online is private
- Separate professional and personal identities
- Review privacy settings regularly
- Protect personal information
- Consider audience and permanence before posting

### 12.9.2 Managing School Accounts – Do's

- Maintain professional tone
- Credit original sources
- Think before responding
- Seek advice when unsure
- Secure accounts properly

12.9.3 Managing School Accounts – Don'ts

- Do not post confidential information
- Do not publish offensive content
- Do not breach copyright or data protection laws
- Do not air internal grievances online

This policy will be reviewed annually and updated as required to reflect changes in technology, legislation and school practice.

## 13. C6 Policy on the use of Artificial Intelligence in Schools

### 13.1 1 Aims and scope

At Bethany School we understand the valuable potential that artificial intelligence (AI), including generative AI, holds for schools. For example, it can be used to enhance pedagogical methods, customise learning experiences and progress educational innovation.

We are also aware of the risks posed by AI, including data protection breaches, copyright issues, ethical complications, safeguarding and compliance with wider legal obligations.

Therefore, the aim of this policy is to establish guidelines for the ethical, secure and responsible use of AI technologies across our whole school community.

This policy covers the use of AI tools by school staff, governors and pupils. This includes generative chatbots such as Co Pilot, ChatGPT and Google Gemini (please note, this list is not exhaustive).

This policy aims to:

- Support the use of AI to enhance teaching and learning
- Support staff to explore AI solutions to improve efficiency and reduce workload
- Prepare staff, governors and pupils for a future in which AI technology will be an integral part
- Promote equity in education by using AI to address learning gaps and provide personalised support
- Ensure that AI technologies are used ethically and responsibly by all staff, governors and pupils
- Protect the privacy and personal data of staff, governors and pupils in compliance with the UK GDPR

### 13.2 1.1 Definitions

This policy refers to both ‘open’ and ‘closed’ generative AI tools. These are defined as follows:

- Open generative AI tools are accessible and modifiable by anyone. They may store, share or learn from the information entered into them, including personal or sensitive information.
- Closed generative AI tools are generally more secure, as external parties cannot access the data you input.

### 13.3 2 Legislation

This policy reflects good practice guidelines/recommendations in the following publications:

- [AI regulation white paper](#), published by the Department for Science, Innovation and Technology, and the Office for Artificial Intelligence
- [Generative artificial intelligence \(AI\) and data protection in schools](#), published by the Department for Education (DfE)

This policy also meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#)
- [Data Protection Act 2018 \(DPA 2018\)](#)

And refers to guidance and advice from:

- [Ethical Guidelines on the Use of AI and Data in Teaching and Learning](#)

### 13.4 3 Regulatory principles

We follow the 5 principles set out in the [AI regulation white paper](#).

REGULATORY PRINCIPLE	WE WILL ...
Safety, security and robustness	<ul style="list-style-type: none"> <li>• Ensure that AI solutions are secure and safe for users and protect users' data</li> <li>• Ensure we can identify and rectify bias or error</li> <li>• Anticipate threats such as hacking</li> </ul>
Appropriate transparency and explainability	<ul style="list-style-type: none"> <li>• Be transparent about our use of AI, and make sure we understand the suggestions it makes</li> </ul>
Fairness	<ul style="list-style-type: none"> <li>• Only use AI solutions that are ethically appropriate, equitable and free from prejudice – in particular, we will fully consider any bias relating to small groups and protected characteristics before using AI, monitor bias closely and correct problems where appropriate</li> </ul>
Accountability and governance	<ul style="list-style-type: none"> <li>• Ensure that the governing board and staff have clear roles and responsibilities in relation to the monitoring, evaluation, maintenance and use of AI</li> </ul>
Contestability and redress	<ul style="list-style-type: none"> <li>• Make sure that staff are empowered to correct and overrule AI suggestions – decisions should be made by the user of AI, not the technology</li> <li>• Allow and respond appropriately to concerns and complaints where AI may have caused error resulting in adverse consequences or unfair treatment</li> </ul>

### 13.5 4 Roles and responsibilities

#### 13.5.1 4.0 AI Champion

Our AI Champion is the Head of Geography. The AI champion works in conjunction with the Senior Management Team (SMT) to promote the use of AI. They are responsible for promoting the use of AI for teacher use to improve teaching and learning and assessment provision.

The day-to-day leadership, ownership and management of AI use in the School is led by the School's SMT.

### 13.5.2 4.1 Governing board

The governing board will:

- Take overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.
- Ensure the headteacher empowers and supports the wider SMT to make informed decisions regarding the effective and ethical use of AI in the school.
- Adhere to the guidelines below to protect data when using generative AI tools:
  - Use only approved AI tools (see section 5 and appendix 1)
  - Seek advice from the Bursar, IT & Head of IT, IT Systems Analyst, SMT the Designated Safeguarding Lead, as appropriate
  - Check whether they are using an open or closed generative AI tool
  - Ensure there is no identifiable information included in what they put into open generative AI tools
  - Acknowledge or reference the use of generative AI in their work
  - Fact-check results to make sure the information is accurate

### 13.5.3 4.2 Headteacher

The headteacher will:

- Work alongside the wider SMT to take responsibility for the day-to-day leadership and management of AI use in the School
- Liaise with the Privacy Compliance Officer (PCO) to ensure that the use of AI is in accordance with data protection legislation
- Liaise with the DSL to ensure that the use of AI is in accordance with Keeping Children Safe in Education and the school's child protection and safeguarding policy
- Ensure that the guidance set out in this policy is followed by all staff
- Ensure that this AI policy is reviewed and updated as appropriate, and at least annually
- Ensure staff are appropriately trained in the effective use and potential risks of AI
- Make sure pupils are taught about the effective use and potential risks of AI
- Sign off on approved uses of AI, or new AI tools, taking into account advice from the Bursar, IT & Head of IT, Safeguarding Lead and wider SMT

### 13.5.4 4.3 Privacy Compliance Officer (DPO)

The Privacy Compliance Officer(PCO) is responsible for monitoring and advising on our compliance with data protection law, including in relation to the use of AI.

Our PCO is the Bursar, Clare Morey: [cmorey@bethanyschool.org.uk](mailto:cmorey@bethanyschool.org.uk)

### 13.5.5 4.4 Designated safeguarding lead (DSL)

The DSL is responsible for monitoring and advising on our compliance with safeguarding requirements including in relation to the use of AI, such as:

- Being aware of new and emerging safeguarding threats posed by AI
- Updating and delivering staff training on AI safeguarding threats
- Responding to safeguarding incidents in line with Keeping Children Safe in Education (KCSIE) and the school's child protection and safeguarding policy
- Understanding the filtering and monitoring systems and processes in place on school

devices The school's DSL is the Deputy Head Pastoral, Alan Sturrock:

[asturrock@bethanyschool.org.uk](mailto:asturrock@bethanyschool.org.uk)

### 13.5.6 4.5 All staff

As part of our aim to reduce staff workload while improving outcomes for our pupils, we encourage staff to explore opportunities to meet these objectives through the use of approved AI tools. Any use of AI must follow the guidelines set out in this policy.

To protect data when using generative AI tools, staff must:

- Use only approved AI tools (see section 5 and appendix 1)
- Seek advice from the Bursar, IT & Head of IT, Safeguarding Lead, SMT as appropriate
- Report safeguarding concerns to the DSL in line with our school's child protection and safeguarding policy
- Check whether they are using an open or closed generative AI tool
- Ensure there is no identifiable information included in what they put into open generative AI tools
- Acknowledge or reference the use of generative AI in their work
- Fact-check results to make sure the information is accurate

All staff play a role in ensuring that pupils understand the potential benefits and risks of using AI in their learning. All of our staff have a responsibility to guide pupils in critically evaluating AI-generated information and understanding its limitations.

### 13.5.7 4.6 Pupils

Pupils must:

- Follow the guidelines set out in section 7 of this policy ('Use of AI by pupils')

## 13.6 5 Staff and governors' use of AI

### 13.6.1 5.1 Approved use of AI

We are committed to helping staff and governors reduce their workload. Generative AI tools can make certain written tasks quicker and easier to complete, but cannot replace the judgement and knowledge of a human expert.

Whatever tools or resources are used to produce plans, policies or documents, the quality and content of the final document remains the professional responsibility of the person who produced it.

Any plans, policies or documents created using AI should be clearly attributed. Any member of staff or governor using an AI-generated plan, policy or document should only share the AI-generated content with other members of staff or governors for use if they are confident of the accuracy of the information, as the content remains the professional responsibility of the person who produced it.

Always consider whether AI is the right tool to use. Just because the school has approved its use doesn't mean it will always be appropriate.

Tools that are approved for school use are detailed in AI Appendix Section 12.1.1

### 13.6.2 5.2 Process for approval

Staff are welcome to suggest new ways of using AI to improve pupil outcomes and reduce workload. Staff should contact the headteacher, AI Champion or another member of SMT to discuss any ideas they may have with regards to using AI, so the headteacher can take the suggestions forward if they deem it to be a satisfactory new method of working.

The headteacher is responsible for signing off on approved uses of AI, or new AI tools, taking into account advice from the Head of IT, SMT, AI Champion, the PCO and data protection impact assessments.

### 13.6.3 5.3 Data protection and privacy

To ensure that personal and sensitive data remains secure, **no one is permitted** to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Bethany School will treat this as a data breach and will follow the personal data breach procedure outlined in our employment manual: *Data Protection Policy*. Please also refer to section 10 of this policy.

### 13.6.4 5.4 Intellectual property

Most generative AI tools use inputs submitted by users to train and refine their models.

Pupils own the intellectual property (IP) rights to original content they create. This is likely to include anything that shows working out or is beyond multiple choice questions.

Pupils' work must not be used by staff to train generative AI models without appropriate consent or exemption to copyright.

Exemptions to copyright are limited – we will seek legal advice if we are unsure as to whether we are acting within the law.

### 13.6.5 5.5 Bias

We are aware that AI tools can perpetuate existing biases, particularly towards protected characteristics including sex, race and disability. For this reason, critical thought must be applied to all outputs of authorised AI applications. This means fact and sense-checking the output.

We will work to identify and rectify bias or error by training staff in this area.

We will also ensure we regularly review our use of AI to identify and correct any biases that may arise.

If parents/guardians or pupils have any concerns or complaints about potential unfair treatment or other negative outcomes as a consequence of AI use, these will be dealt with through our [complaints procedure](#).

### 13.6.6 5.6 Raising concerns

We encourage staff and governors to speak to the headteacher in the first instance if they have any concerns about a proposed use of AI, or the use of AI that may have resulted in errors that lead to adverse consequences or unfair treatment.

Safeguarding concerns arising from the use of generative AI must be reported immediately to the DSL in accordance with our School Safeguarding and Child Protection policy.

### 13.6.7 5.7 Ethical and responsible use

We will always:

- Use generative AI tools ethically and responsibly
- Work to ensure that AI use does not reinforce bias, and enables everyone to participate equally and fairly
- Consider whether the tool has real-time internet access, or access to information up to a certain point in time, as this may impact the accuracy of the output
- Fact and sense-check the output before relying on it

Staff and governors must not:

- Generate content to impersonate, bully or harass another person
- Generate explicit or offensive content
- Input offensive, discriminatory or inappropriate content as a prompt

## 13.7 6 Educating pupils about AI

At Bethany School we acknowledge that pupils benefit from a knowledge-rich curriculum that allows them to become well-informed users of technology and understand its impact on society. Strong foundational knowledge will ensure that pupils develop the right skills to make the best use of generative AI.

Both within our PSHCE curriculum and in the wider curriculum, pupils are taught about the potential benefits of using AI tools to aid their learning, while also covering subjects such as:

- Creating and using digital content safely and responsibly

Page 64 of 69

---

File name:	Online Safety Policy	Version	1.0
Author	Katja Thornton	Issue date	16/02/2026
Authorised by	Alan Sturrock	Review date	February 2027

**This is a controlled document. If printed it may no longer be valid. The current master version is held in the Staff Team under School Policies**

- The limitations, reliability and potential bias of generative AI
- Online safety to protect against harmful or misleading content

### 13.8 7 Use of AI by pupils

We recognise that AI has many uses to help pupils learn.

Pupils may use AI tools for certain tasks, as directed and advised by their teachers. For example:

- As a research tool to help them find out about new topics and ideas.
- When specifically studying and discussing AI in schoolwork, for example in IT lessons or art homework about AI-generated images.
- To support revision through the generation of example questions and responses.

All AI-generated content must be properly attributed and appropriate for the pupils' age and educational needs.

AI may also lend itself to cheating and plagiarism. To mitigate this, pupils must:

- Follow guidance when completing formal assessments, NEA and coursework tasks as detailed in the School Malpractice Policy.
- Pupils must never attempt to present AI generated work as their own. This list of AI misuse is not exhaustive.

Where AI tools are used as a source of information, pupils should reference their use of AI. The reference must show the name of the AI source and the date the content was generated.

When it is discovered that pupils have used AI to cheat, we will follow plagiarism procedures as set out in our Malpractice Policy and with reference to our Behaviour and Discipline Policy.

Pupils must consider what is ethical and appropriate in their use of AI and must not:

- Generate content to impersonate, bully or harass another person.
- Generate or share explicit or offensive content, including, but not limited to, generating inappropriate or sexualised images of pupils.
- Input offensive, discriminatory or inappropriate content as a prompt.

### 13.9 8 Formal assessments

We will continue to take reasonable steps where applicable to prevent malpractice involving the use of generative AI in assessments. See our Non-Examination Assessment Policy and Malpractice Policy for further details.

We will follow the latest guidance published by the Joint Council for Qualifications (JCQ) on [AI use in assessments](#).

### 13.10 9 Staff training

We will ensure that staff are kept up to date with developments in AI through staff briefings and training days. We will ensure that:

- AI is a regular agenda item in IT and Education Committees, Middle Leader and Department meetings.
- AI use is included in staff training about safe internet use and online safeguarding
- Wider Continuing professional development (CPD) opportunities about AI are shared with staff

### 13.11 10 Referral to our child protection and safeguarding policy

The school is aware that the use of generative AI may in some circumstances lead to safeguarding concerns including, but not limited to:

- Sexual grooming
- Sexual harassment
- Sexual extortion
- Child sexual abuse/exploitation material
- Harmful content
- Harmful advertisements and promotions
- Bullying

Where there are safeguarding concerns arising from the use of generative AI, a report must be made to the DSL immediately.

Any such incident will be dealt with reference to the School [Safeguarding and Child Protection](#), [Anti-Bullying](#), [Behaviour and Discipline](#) policies and the Online Safety Policy.

### 13.12 11 Breach of this policy

#### 13.12.1 11.1 By staff

Breach of this policy by staff will be dealt with in line with our staff code of conduct. Where disciplinary action is appropriate, it may be taken whether the breach occurs:

- During or outside of working hours
- On an individual's own device or a school device
- At home, at school or from a remote working location

Staff members will be required to co-operate with any investigation into a suspected breach of this policy. This may involve providing us with access to:

- The generative AI application in question (whether or not it is one authorised by the school)
- Any relevant passwords or login details

You must report any breach of this policy, either by you or by another member of staff, to the headteacher immediately.

#### 13.12.2 11.2 By governors

It is expected that governors will follow the same guidelines as staff in respect of AI use.

#### 13.12.3 11.3 By pupils

Any breach of this policy by a pupil will be dealt with in line with our [Behaviour and Discipline](#) policy and with reference to our [Safeguarding and Child Protection](#), [Anti-Bullying](#), Online Safety policies as appropriate.

**13.13 12 Monitoring and transparency**

AI technology, and the benefits, risks and harms related to it, evolves and changes rapidly. Consequently, this policy is a live document that must be kept updated by SMT and Educational Committee whenever there is a significant change to either AI use by the school or the associated risks of AI usage.

This policy will also be reviewed annually and updated to align with emerging best practices, technological advancements and changes in regulations.

All teaching staff are expected to read and follow this policy. The Headteacher is responsible for ensuring that the policy is followed.

The SMT will monitor the effectiveness of AI usage across the school.

We will ensure we keep members of the school community up to date on the use of AI technologies for educational purposes. As part of our regular surveys, feedback from pupils, parents/guardians and staff will be considered in the ongoing evaluation and development of AI use in school.

**13.14 12.1.1 AI Appendix 1: Approved uses of AI tools (table)**

Note that open-source AI tools / open AI tools, meaning tools that anyone can access and modify, should only be used for tasks that don't require personal information to be input.

APPROVED AI TOOLS	APPROVED FOR	APPROVED USES
ChatGPT Google Gemini	<ul style="list-style-type: none"> <li>• Teachers</li> <li>• Governors</li> <li>• Support staff</li> <li>• Sixth form and pupils in Years 10 &amp; 11 with guidance and education</li> </ul>	<ul style="list-style-type: none"> <li>• Administrative support – such as: drafting letters / e-mails / structuring formal reports</li> <li>• Supporting the generation of lesson plans, materials and ideas</li> <li>• Supporting revision and reviewing of work under teacher guidance and instruction</li> </ul>

---

File name:	Online Safety Policy	Version	1.0
Author	Katja Thornton	Issue date	16/02/2026
Authorised by	Alan Sturrock	Review date	February 2027

APPROVED AI TOOLS	APPROVED FOR	APPROVED USES
Co Pilot	<ul style="list-style-type: none"> <li>• Teachers</li> <li>• Governors</li> <li>• Support staff</li> <li>• Sixth form and pupils in Years 9-11 with guidance and education</li> </ul>	<ul style="list-style-type: none"> <li>• Administrative support – such as: drafting letters / e-mails / structuring formal reports</li> <li>• Supporting the generation of lesson plans, materials and ideas</li> <li>• Supporting revision and reviewing of work under teacher guidance and instruction</li> </ul>
Gamma	<ul style="list-style-type: none"> <li>• Teachers</li> <li>• Support staff</li> </ul>	<ul style="list-style-type: none"> <li>• Supporting the generation of presentations</li> </ul>
Tutor2U	<ul style="list-style-type: none"> <li>• Teachers</li> <li>• Pupils</li> </ul>	<ul style="list-style-type: none"> <li>• Supporting revision</li> <li>• Supporting feedback and assessment</li> </ul>
Photomath	<ul style="list-style-type: none"> <li>• Teachers</li> <li>• Pupils</li> </ul>	<ul style="list-style-type: none"> <li>• Supporting revision and learning</li> </ul>
Grammarly	<ul style="list-style-type: none"> <li>• Teachers</li> <li>• Pupils</li> </ul>	<ul style="list-style-type: none"> <li>• Supporting report writing</li> <li>• Checking writing but not when submitted for formal assessment where this is not permitted</li> </ul>
Ollama	<ul style="list-style-type: none"> <li>• Teachers</li> </ul>	<ul style="list-style-type: none"> <li>• Administrative support – such as: drafting letters / e-mails / structuring formal reports / managing data</li> <li>• Supporting the generation of lesson plans, materials and ideas</li> <li>• Supporting revision and reviewing of work under teacher guidance and instruction</li> </ul>