BROWNEDGE ST MARY'S CATHOLIC HIGH SCHOOL

BROWNEDGE ST MARY'S
CATHOLIC HIGH SCHOOL
'Let your light shine'

Online Safety Policy including AI Policy

Approved by Full Governing Body	Date: December 2025

Signature of Head Teacher/Chair of Governors:	Date:

Policy amended by: N Oddie	Date: December 2025	Review Date: December 2027

Contents

Let Your Light Shine

If we love others, we live in the light. 1 John 2:10

Inspired by our Gospel Values, we have a shared responsibility to

- create an environment of welcome, love and respect for each member of our learning family.
- develop the unique gifts and talents of all, striving for excellence in everything we do.
- live out our commitment to love, service and justice in the local and global community.
- nurture the journey of faith and discovery for all
- celebrate and reflect on the love of God which is at the heart of all we are.

1. Aims

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This e-safety policy should help to ensure safe and appropriate use.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school.

Our school aims to:

- ➢ Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- ➢ Identify and support groups of pupils that are potentially at greater risk of harm online than others
- ➢ Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- ➢ Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- ➢ **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- ➢ **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes
- ➢ **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- ➢ **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

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

> Teaching online safety

> Meeting digital and technology standards

> https://www.gov.uk/government/publications/preventing-and-tackling-bullyingPreventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

> Relationships and sex education (RSE) and health education

> Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

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

3. Roles and responsibilities

3.1   The governing board

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

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

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

The governing board will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The governing board will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

> Identifying and assigning roles and responsibilities to manage filtering and monitoring systems

> Reviewing filtering and monitoring provisions at least annually

> Blocking harmful and inappropriate content without unreasonably impacting teaching and learning

> Having effective monitoring strategies in place that meet the school's safeguarding needs

The governor who oversees online safety is our Safeguarding Leads – Mrs Fordyce and Mr Williams

The governor who oversees cybersecurity is Mr Cartmell

All governors will:

> Ensure they have read and understand this policy.

> Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2).

> Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures.

> Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is

because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

3.2   The headteacher

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

> The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the Lead DSL and Network Manager.

> The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

3.3   The designated safeguarding lead

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

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

> Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.

> Working with the headteacher and governing board to review this policy every two years and ensure the procedures and implementation are updated and reviewed regularly.

> Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.

> Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly

> Working with the ICT manager to make sure the appropriate systems and processes are in place.

> Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents.

> Managing all online safety issues and incidents in line with the school's child protection policy.

> Responding to safeguarding concerns identified by filtering and monitoring

> Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.

> Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.

> Updating and delivering staff training on online safety (appendix 6) contains a self-audit for staff on online safety training needs).

> Liaising with other agencies and/or external services if necessary.

> Providing regular reports on online safety in school to the headteacher and/or governing board.

> Undertaking annual risk assessments that consider and reflect the risks children face.

> Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

> Ensuring that any online safety incidents are logged on CPOMs

This list is not intended to be exhaustive.

3.4   The Network manager

The Network manager is responsible for:

> Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

- Conducting a full security check and monitoring the school's ICT systems on a weekly basis

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

- Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

- Keeping 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

This list is not intended to be exhaustive. More information regarding technical security can be found in appendix 5

3.5   All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy

- Implementing this policy consistently

- Agreeing and adhering to the terms on acceptable use of the school's Staff Acceptable Use Policy (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)

- If signed the extended Internet Filtering Agreement, agree to take responsibility for any websites that they visit and they understand that there is a chance that they may be able to access some websites that may contain inappropriate content. They must take on the responsibility of checking websites for inappropriate material prior to using in lesson

- That their laptop/PC is left locked when not in use to ensure there is no risk of students being able to access inappropriate material.

- Digital communications with pupils (email/Firefly/voice) should be on a professional level and only carried out using official school systems.

- Digital communications with pupils (email/Firefly/voice) should be on a professional level and only carried out using official school systems.

- Knowing that the DSL is responsible for the filtering and monitoring systems and processes and being aware of how to report any incidents of those systems or processes failing via CPOMs.

- Following the correct procedures by liaising with ICT support team if they need to bypass the filtering and monitoring systems for educational purposes.

- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy.

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

3.6   Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

- Read and agree to the Parent/Carer acceptable use agreement (appendix 4)

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

o   What are the issues? – UK Safer Internet Centre

o   Hot topics – Childnet International

o   Parent resource sheet – Childnet International

3.7   Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

4.1   Pupils will be taught about online safety as part of the curriculum

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

Specific teaching will take place through the teaching of the National Curriculum computing programmes of study and in our Relationships and sex education and health education provision. Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities.

In **KS3**, pupils will be taught to:

> Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy

> Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **KS4** will be taught:

> To understand how changes in technology affect safety, including new ways to protect their online privacy and identity

> How to report a range of concerns

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

> Rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online

> Online risks, including the importance of being cautious about sharing personal information online and of using privacy and location settings appropriately to protect information online. Pupils should also understand the difference between public and private online spaces and related safety issues

> The characteristics of social media, including that some social media accounts are fake, and / or may post things which aren't real / have been created with AI. That social media users may say things in more extreme ways than they might in face-to-face situations, and that some users present highly exaggerated or idealised profiles of themselves online

> Not to provide material to others that they would not want to be distributed further and not to pass on personal material which is sent to them. Pupils should understand that any material provided online might be circulated, and that once this has happened there is no way of controlling where it ends up. Pupils should understand the serious risks of sending material to others, including the law concerning the sharing of images

> That keeping or forwarding indecent or sexual images of someone under 18 is a crime, even if the photo is of themselves or of someone who has consented, and even if the image was created by the child and/or using AI-generated imagery. Pupils should understand the potentially serious consequences of acquiring or generating indecent or sexual images of someone under 18, including the potential for criminal charges and severe penalties including imprisonment. Pupils should know how to seek support and should understand that they will not be in trouble for asking for help, either at school or with the police, if an image of themselves has been shared. Pupils should also understand that sharing indecent images of people over 18 without consent is a crime

> What to do and how to report when they are concerned about material that has been circulated, including personal information, images or videos, and how to manage issues online

> About the prevalence of deepfakes including videos and photos, how deepfakes can be used maliciously as well as for entertainment, the harms that can be caused by deepfakes and how to identify them

> That the internet contains inappropriate and upsetting content, some of which is illegal, including unacceptable content that encourages misogyny, violence or use of weapons. Pupils should be taught where to go for advice and support about something they have seen online. Pupils should understand that online content can present a distorted picture of the world and normalise or glamorise behaviours which are unhealthy and wrong

> That social media can lead to escalations in conflicts, how to avoid these escalations and where to go for help and advice

> How to identify when technology and social media is used as part of bullying, harassment, stalking, coercive and controlling behaviour, and other forms of abusive and/or illegal behaviour and how to seek support about concerns

> That pornography, and other online content, often presents a distorted picture of people and their sexual behaviours and can negatively affect how people behave towards sexual partners. This can affect pupils who see pornographic content accidentally as well as those who see it deliberately. Pornography can also portray misogynistic behaviours and attitudes which can negatively influence those who see it

> How information and data is generated, collected, shared and used online

> That websites may share personal data about their users, and information collected on their internet use, for commercial purposes (e.g. to enable targeted advertising)

> That criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion

> That AI chatbots are an example of how AI is rapidly developing, and that these can pose risks by creating fake intimacy or offering harmful advice. It is important to be able to critically think about new types of technology as they appear online and how they might pose a risk

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

4.2   Pupils will be taught practical cyber security skills

All pupils will receive age-appropriate training on safe internet use, including:

> Methods that hackers use to trick people into disclosing personal information

> Password security

> Social engineering

> The risks of removable storage devices (e.g. USBs)

> Multi-factor authentication

> How to report a cyber incident or attack

> How to report a personal data breach

Pupils will also receive age-appropriate education on safeguarding issues such as cyberbullying and the risks of online radicalisation.

5. Educating the school community

5.1   Parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website or via Firefly. This policy will also be shared with parents/carers.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

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

5.2   Staff/volunteers and governors about online safety

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

> a planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly

> all new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements

> the online safety coordinator/officer (or other nominated person) will receive regular updates through attendance at external training events, (e.g. from Consortium/ LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations

> this online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days

> the online safety coordinator/officer (or other nominated person) will provide advice/guidance/training to individuals as required.

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

> attendance at training provided by the local authority/National Governors Association/or other relevant organisation

> participation in school training/information sessions for staff or parents.

6. Cyber-bullying

6.1   Definition

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

6.2   Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The 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 e-safety behaviour that take place out of school.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes our Learning for Life education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school anti-bullying and behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3   Examining electronic devices

The headteacher, and any member of staff authorised to do so, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

> Poses a risk to staff or pupils, and/or

> Is identified in the school rules as a banned item for which a search can be carried out, and/or

> Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

> Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher.

> Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it

> Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

> Cause harm, and/or

> Undermine the safe environment of the school or disrupt teaching, and/or

> Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction members of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

> They reasonably suspect that its continued existence is likely to cause harm to any person, and/or

> The pupil and/or the parent/carer refuses to delete the material themselves

> If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

   o **Not** view the image

   o Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:
> The DfE's latest guidance on searching, screening and confiscation

> UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

> Our behaviour policy

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

6.4   Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Brownedge St Mary's recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Brownedge St Mary's will treat any use of AI to bully pupils very seriously, in line with our behaviour/anti bullying policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

Any use of artificial intelligence should be carried out in accordance with our AI usage policy. (See Appendix 7)

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use, if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Mobile technologies

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school policies including but not limited to those for safeguarding, behaviour, anti-bullying, acceptable use, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school learning platform and other cloud-based services such as e-mail and data storage.

Mobile Phones

> Pupils – if pupils bring mobile phones into school they MUST be handed into the Form Tutor at Registration to be

> locked in the mobile phone safe. Pupils caught with mobile phones (whether they are on or off) will receive sanctions. (See behaviour Policy)

> Staff – Staff should not use their mobile phones whilst performing their professional duties. (See Staff Codie of Conduct)

Mobile school/work devices
In preparing this policy, the school considers possible issues and risks, which include:
> security risks in allowing connections to the school network

> filtering of personal devices

> breakages and insurance

> access to devices for all pupils

> avoiding potential classroom distraction

> network connection speeds, types of devices

> charging facilities

> total cost of ownership

In addition to the points above, the school Acceptable Use Agreements for staff, pupils, parents and carers will give consideration to the use of mobile technologies.

	School devices			Personal devices	
	School owned for individual use	School owned for multiple users	Authorised device[1]	Pupil owned	Staff owned
Allowed in school	Yes	Yes	Yes	No	Limited[2]
Full network access	Yes	Yes	Limited	No	No
Internet only	N/A	N/A	N/A	No	Yes

[1] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.
[2] Staff personal device are permitted in school for emergency use only and have restricted internet only access where requested for school use

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). The devices must not be used in any way that would violate the school's terms of acceptable use. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

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

All members using a mobile device for school purposes will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

> Keeping the device password-protected – strong passwords can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager

> Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device

> Making sure the device locks if left inactive for a period of time

> Not sharing the device among family or friends

> Keeping operating systems up to date by promptly installing the latest updates

If there are any concerns over the security of any device, the individual must seek advice from the ICT Manager.

9. Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

> When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.

> Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should be taken on school equipment; the personal equipment of staff will only be used with the agreement of the Headteacher. Once digital /video images have been uploaded onto the school network they should be deleted from any equipment. Only members of staff who have signed an enhanced Digital/Video Image Use Agreement can personally store and manipulate images/videos.

> Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

> Pupils must not take, use, share, publish or distribute images of others without their permission

> Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

> Pupils' full names will not be used anywhere on a website in association with photographs.

> Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (may be covered as part of the AUP signed by parents or carers at the start of the year)

10. Communication Technologies

10.1   A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

Communication Technologies	Staff & other adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓					✓		
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time	✓							✓
Taking photos on mobile phones or other camera devices not belonging to school			✓					✓
Use of other mobile devices e.g. tablets, gaming devices				✓				✓
Use of personal email addresses in school, or on school network	✓							✓
Use of school email for personal emails *				✓				✓

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

> the official school e-mail service may be regarded as safe and secure and is monitored. Users should be aware that e-mail communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems

> users must immediately report to a member of the ICT Support Team or relevant member of staff (e.g. SLT, Head of House, Head of Faculty) – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication

> any digital communication between staff and pupils or parents/carers (e-mail, chat, learning platform, etc.) must be professional in tone and content. These communications may only take place on official (monitored)

school systems. Personal e-mail addresses, text messaging or social media must not be used for these communications

> pupils are taught about online safety issues, such as the risks attached to the sharing of personal details. They are taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies

> personal information should not be posted on any internet platform and only official e-mail addresses should be used to identify members of staff.

10.2   Social media

Expectations for teachers' professional conduct are set out by the Department for Education (DfE,) but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. All staff working at any educational establishment are expected to demonstrate a professional approach and respect for pupils and their families and for colleagues and the learning setting.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils through:
> ensuring that personal information is not published

> training being provided including acceptable use, social media risks, checking of settings, data protection and reporting issues

> clear reporting guidance, including responsibilities, procedures and sanctions

> risk assessment, including legal risk.

School staff should ensure that:
> no reference should be made in social media to pupils, parents and carers or school staff

> they do not engage in online discussion on personal matters relating to members of the school community

> personal opinions should not be attributed to the school or local authority

> security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

When official school social media accounts are established there should be:
> a process for approval by senior leaders

> clear processes for the administration and monitoring of these accounts – involving at least two members of staff

> a code of behaviour for users of the accounts

> systems for reporting and dealing with abuse and misuse

> understanding of how incidents may be dealt with under school disciplinary procedures.

Personal use
> Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

> Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

> Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

> The school permits reasonable and appropriate access to private social media sites.

Monitoring of public social media

> As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.

> The school should effectively respond to social media comments made by others according to a defined policy or process.

School use of social media for professional purposes will be checked regularly by a senior leader and online safety group to ensure compliance with the social media, data protection, communications, digital image and video policies.

Unsuitable/inappropriate activities

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

11. Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation. The school must ensure that:

> it has a Data Protection Policy

> it implements the data protection principles and is able to demonstrate that it does so

> it has paid the appropriate fee Information Commissioner's Office (ICO)

> it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest. The school may also wish to appoint a Data Manager and Systems Controllers to support the DPO

> it has an 'information asset register' in place and knows exactly what personal data it holds, where, why and which member of staff has responsibility for managing it

> the information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed

> it will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. The school is developing and implementing a "retention schedule" to support this

> data held must be accurate and up to date where this is necessary for the purpose it is held and systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals

> it provides staff, parents, volunteers, teenagers and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice

> procedures must be in place to deal with the individual rights of the data subject, e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them

> Data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier

> IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems

> it has undertaken appropriate due diligence and has GDPR compliant contracts in place with any data processors

> it understands how to share data lawfully and safely with other relevant data controllers

> there are clear and understood policies and routines for the deletion and disposal of data

> it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In

order to do this it has a policy for reporting, logging, managing, investigating and learning from information risk incidents

> all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

> data must be encrypted and password protected

> device must be password protected

> device must be protected by up to date virus and malware checking software

> data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

> at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse

> can recognise a possible breach, understand the need for urgency and know who to report it to within the school

> can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school

> only use encrypted mobile devices (including USBs) for personal data, particularly when it is about children

> will not transfer any school personal data to personal devices except as in line with school policy

> use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" or "locked" at the end of any session in which they are using personal data

> transfer data using encryption and secure password protected devices.

12. How the school will respond to issues of misuse

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

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

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

13. Training for staff, governors and volunteers

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

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

> Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

> Children can abuse their peers online through:

- Abusive, threatening, harassing and misogynistic messages

- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups

- Sharing of abusive images and pornography, to those who don't want to receive such content
  - Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

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

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

Volunteers will receive appropriate training and updates, if applicable.

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

14. Monitoring arrangements

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

This policy will be reviewed once every two years by the DLS. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

15. Links with other policies

This online safety policy is linked to our:

- Behaviour policy
- Staff Code of Professional Conduct
- Data protection policy and privacy notices
- Complaints procedure
- Safeguarding and Child Protection Policy
- Acceptable Use of the Internet Policy
- Remote Learning Policy
- Guidance for Safer Working Practice for Adults who Work with Children and Young People (DcSF May 2022)

Appendix One

Pupil Acceptable User Agreement

Acceptable User Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:
- I understand that the school will monitor my use of systems, devices and other digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I will not write down or store a password where it is possible that someone may steal it
- I will be aware of "stranger danger", when I am communicating online
- I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details, etc.)
- I will not arrange to meet people off-line that I have communicated with online
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online

I understand that everyone has equal rights to use technology as a resource and:
- I understand that the school ICT systems are primarily intended for educational use and that I will not I understand that the school systems and devices are primarily intended for educational use and that I will only use them for personal or recreational use if I have permission
- I will only make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work, if I have permission
- I will only use the school systems or devices for online gaming, internet shopping/e-commerce, file sharing, or video broadcasting (e.g. YouTube), if I have permission of a member of staff to do so.

I will act as I expect others to act toward me:
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- 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 **take** or **share** (distribute) images or videos of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:
- I will only use my device(s) in school if I have permission. I understand that, if I do use my device(s) in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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 damage or faults involving equipment or software, however this may have happened
- I will only open hyperlinks in emails or attachments to emails, if I know and trust the person/organisation who sent the email, and have no concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will only install/ store programmes on a device, if I have permission and this software will not impact on the ability to use the device for learning
- I will only use social media sites with permission and at the times that are allowed

When using the internet for research or recreation, I recognise that:
- o I should ensure that I have permission to use the original work of others in my own work
- o Where work is protected by copyright, I will not download copies (including music and videos)
- o When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

Generative AI (GenAI) is a type of artificial intelligence (AI) that creates new content, such as text, images, videos and music, based on large amounts of existing information. We want you to be able to use AI as a helpful tool for your learning. You must also be aware of the risks of using AI, and the rules you must follow to be a responsible and safe AI user. When using AI in school, I recognise that:
- o I will only use AI tools that my school or teacher has approved, and only for learning.
- o I will make sure all work I submit is genuinely my own, and I will not use AI to cheat, deceive, or pretend AI-generated work is human-made. If it is AI generated, I will acknowledge any AI use and reference its source.
- o I will remember that AI can be unreliable, biased, or incorrect, and I will double-check any information it gives me using trusted sources.
- o I will not share or forward AI-generated information unless I know it is accurate, appropriate, and safe.
- o I will not enter personal information, images, documents, or sensitive details—mine or anyone else's—into AI tools, because they may store or learn from what I upload.
- o I will use AI ethically: being fair, honest, respectful, and aware of the impact my choices can have on others.
- o I will not use AI to create or share harmful, offensive, inappropriate, misleading, or illegal content, including misinformation, disinformation, or material that breaks copyright.
- o I will not use AI to imitate or misrepresent myself or another person.
- o I will not rely on AI for personal, emotional, or wellbeing advice and I will speak to a trusted adult if I need support.
- o I will report any worrying, unsafe, or harmful AI content to a member of staff straight away.

I understand that I am responsible for my actions, both in and out of school:
- o I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- o I understand that if I fail to comply with this Acceptable User Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections below to show that you have read, understood and agree to the rules included above. If you do not sign and return this agreement, access will not be granted to school systems and devices.

I have read and understand the above and agree to follow these guidelines when:

- • I use the school ICT systems and devices (both in and out of school)

- • I use my own devices in school when allowed

- • I use my own equipment out of school in a way that is related to me being a member of this school eg communicating with other members of the school, accessing school email, website etc.

Name of Pupil	
Form	

19

Appendix Two

Staff and Volunteer Acceptable Use Policy Agreement

Acceptable Use Agreement

I understand that I must use school digital technologies in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:
- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, Remote Access, online platforms) out of school.
- I understand that the school systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications/use of digital/video images and actions when using school ICT systems:
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- 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. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not post or publish any material on an external website or social networking site (e.g. Facebook, Twitter) that is inappropriate or brings the school into disrepute. This includes any reference to Brownedge St Mary's, it's staff or students. If you are in any doubt as to what is appropriate, do not post the material and consult your line manager.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not share personal mobile numbers, email addresses or personal web space details to any pupil.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:
- When I use my mobile devices/laptops/mobile phones /USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices, especially USB devices, are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not deliberately upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials. (e.g. illegal WIFI access)
- I will sign the extended Internet Filtering Agreement, agreeing to take responsibility for any websites that are visited, understanding there is a chance that they may be able to access some websites that may contain

inappropriate content and take responsibility for checking websites for inappropriate material prior to using in a lesson.

- o I understand that the DSL is responsible for the filtering and monitoring systems and processes and I am aware of how to report any incidents of those systems or processes failing via CPOMs.
- o I will follow the correct procedures by liaising with ICT support team if I need to bypass the filtering and monitoring systems for educational purposes.
- o I will work with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- o I will respond appropriately to all reports and concerns about online sexual violence and/or harassment, and maintain an attitude of 'it could happen here'.
- o I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- o I will not disable or cause any damage to school equipment, or the equipment belonging to others. I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- o I understand that the data protection policy requires any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- o I will either lock or log off my workstation/Laptop/iPad when away from my desk to ensure data is kept private and confidential and that I will not view emails or staff/student information on a staff workstation when connected to a projector/whiteboard
- o I will immediately report any damage or faults involving equipment or software, however this may have happened.

Generative AI can be a valuable tool to support teaching, planning, and administration. However, staff must use AI safely, ethically and in line with legal and safeguarding expectations. The following guidance outlines the standards all staff must follow when using AI in school.

- o I will use AI tools professionally and responsibly to support planning, ensuring that all decisions, judgements and final plans are based on my own expertise rather than AI. Where possible, I will ensure my settings in Open generative platforms are set not to share my data to train any models.
- o I will protect data by not entering personal, sensitive, or identifiable information into AI tools unless they are officially confirmed as GDPR-compliant, and I will check AI-generated content for accidental sensitive information.
- o I will use AI safely and responsibly by avoiding harmful, inappropriate, biased, or discriminatory content, and I will report any concerning AI output to safeguarding or digital safety leads.
- o I will ensure that my use of AI never compromises pupil safety, wellbeing, safeguarding expectations, or the core values and professionalism of the school.
- o I will verify and critically check all AI-generated information before using it, recognising that AI can be inaccurate, biased, or misleading, and I will not use it to determine grades or assessment decisions without validating the output myself.
- o I will be transparent with pupils when AI has supported teaching materials and will ensure that AI use supports learning without undermining academic integrity or exam regulations.
- o I will model ethical AI use, guide pupils in using AI safely and responsibly, challenge misuse, and ensure that AI enhances my practice without replacing planning, pedagogy, or professional accountability.
- o I will use AI to streamline administrative tasks where appropriate, but I will not allow it to replace meaningful planning, preparation, or pedagogical thinking.
- o I will ensure that AI enhances my practice in a positive and balanced way, without reducing teaching quality, accuracy, or my professional accountability.

I understand that I am responsible for my actions in and out of school:
- o I understand that this Acceptable Use Agreement applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- o I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the Staff and Volunteer Acceptable Use Agreement and agree to use the school digital technology 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.

Staff / Volunteer Name

Signed

Date

Appendix Three

Acceptable Use Agreement for guests / visitors

This Acceptable Use Agreement is intended to ensure:
➢ that guests/visitors of school digital technologies will be responsible users and stay safe while using these systems and devices
➢ that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
➢ that users are protected from potential risk in their use of these systems and devices.

Acceptable Use agreement
o I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school.
o I understand that my use of school systems and devices and digital communications will be monitored.
o I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
o I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, 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.
o I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
o I will not access, copy, remove or otherwise alter any other user's files, without permission.
o I will ensure that if I take and/or publish images of others I will only do so with their permission and in line with school policies. 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.
o 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.
o 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.
o 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.
o I will not disable or cause any damage to school equipment, or the equipment belonging to others.
o I will immediately report any damage or faults involving equipment or software, however this may have happened.
o I will ensure that I have permission to use the original work of others in my own work.
o Where work is protected by copyright, I will not download or distribute copies (including music and videos).
o I will only use pupil AI tools approved by the school and follow all guidance provided about their safe and appropriate use.
o I will not enter personal data, pupil information, images, or sensitive documents into AI tools, and I will ensure any AI-generated content protects confidentiality.
o I will avoid generating or using harmful, inappropriate, misleading, or biased AI content, and I will report any concerning output to school staff immediately.
o I will ensure that my use of AI never compromises pupil safety, wellbeing, or safeguarding expectations.
o I will act responsibly and professionally when using AI, relying on my own judgement and being transparent with staff if AI supported any information or materials I share.
o 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 digital technology 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.

Name _____ Signed _____ Date _____

Appendix Four

Parent/Carer Acceptable Use Agreement

Internet, AI and Digital Technology Use

As the parent / carer I give permission for my son / daughter to have access to the internet and to digital technology systems at school.

I know that my son / daughter has signed or will sign an Acceptable Use Agreement and has 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 digital technology systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the digital technology 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 understand that my son/daughter may use age-appropriate and school-approved artificial intelligence (AI) tools to support their learning. I know that the school will teach pupils how to use AI safely, responsibly, and critically, and that my child will be expected to follow the school's AI Acceptable Use guidance.

I understand that AI tools can sometimes provide inaccurate, biased, or inappropriate information, and I will encourage my child to check information carefully and to speak to a trusted adult if they are unsure. I also understand that pupils are not permitted to enter personal information, images, or sensitive details into AI systems, and that the school will contact me if they have concerns about my child's use of AI.

I will support the school by encouraging my child to use AI safely and ethically at home and by raising any concerns about AI use or online safety with the school as soon as possible.

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.

Student / Pupil Name	
Parent / Carers Name	
Signed	
Date	

Use of Digital/Video Images

As the parent / carer I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at, or of, school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Student / Pupil Name	
Parent / Carers Name	
Signed	
Date	

Use of Cloud Systems Permission Form

The school uses a variety of digital platforms, for example, Microsoft 365, MSTeams, Firefly, Talaxy, GCSEPod, Seneca, Quizlet and Sparx, for pupils and staff. This is not an exhaustive list. The above services are available to each pupil as part of the school's online presence.

Using these services will enable your child to collaboratively create, edit and share files and websites for school related projects and communicate via email with other pupils and members of staff. These services are entirely online and available 24/7 from any internet-connected computer.

The school believes that use of the tools significantly adds to your child's educational experience.

Please refer to the school's latest Data Protection Policy for more information.

I consent to my child having access to these services.

Student / Pupil Name	
Parent / Carers Name	
Signed	
Date	

School Technical Security Policy
(including filtering and passwords)

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be 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
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies)
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of The Network Manager.

Technical Security

Policy statements

The school will be 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
- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling must be securely located and physical access restricted
- appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data
- responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff
- all users will have clearly defined access rights to school technical systems defined by their role as a member of staff or as a pupil
- 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 Network Manager 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
- mobile device security and management procedures are in place
- school technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement
- remote management tools are used by staff to control workstations and view users activity
- an appropriate system is in place for users to report any actual/potential technical incident to the online safety co-ordinator/network manager/technician
- an agreed policy is in place for the provision of temporary access of guests / visitors, (e.g. trainee teachers, supply teachers, visitors) onto the school system
- an agreed policy is in place within respective policies regarding the downloading of executable files and the installation of programmes on school devices by users
- an agreed policy is in place within respective policies regarding the extent of personal use that users (staff/pupils/guests/visitors) and their family members are allowed on school devices that may be used out of school
- an agreed policy is in place in line with the schools GDPR policy regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices
- the school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.
- personal data should not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Password Security

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.

Policy Statements:
These statements apply to all users.
➢ All school networks and systems will be protected by secure passwords.
➢ All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually
➢ All users (adults and pupils) have responsibility 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.
➢ Passwords must not be shared with anyone.
➢ All users will be provided with a username and password by the ICT Team who will keep an up to date record of users and their usernames.

Password requirements:
Staff Passwords should be a minimum 8 Characters with a mixture of upper and lower case, including at least one number or special character. Passwords must be changed on first login to the system.

Pupil passwords:
➢ Records of pupil usernames and passwords are securely kept when not required by the user.
➢ Passwords will be required to change if it is thought to be compromised.
➢ Pupils will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

Notes for technical staff/teams
➢ Each administrator should have an individual administrator account, as well as their own user account with access levels set at an appropriate level. Consideration is also be given to using two factor authentication for such accounts.
➢ There are multiple redundancies to gain domain admin level access to the network, should this be required.
➢ It is good practice that where passwords are used there is a user-controlled password reset process to enable independent, but secure re-entry to the system. This ensures that only the owner has knowledge of the password.
➢ Where user-controlled reset is not possible, passwords for new users, and replacement passwords for existing users will be allocated by the ICT Team
➢ This password is temporary and the user is forced to change their password on first login. The generated passwords should also be long and random.
➢ Requests for password changes should be authenticated by ICT Team to ensure that the new password can only be passed to the genuine use.
➢ Suitable arrangements are in place to provide guests/visitors/supply with appropriate access to systems which expires after use.
➢ In good practice, the account is "locked out" for an amount of time following six successive incorrect log-on attempts.

Training/Awareness: Members of staff will be made aware of the school password policy:
➢ at induction
➢ through the school's online safety policy and password security policy
➢ through the acceptable use agreement.

Pupils will be made aware of the school's password policy:
➢ in Computing lessons by teachers
➢ through the Acceptable Use Agreement.

Audit/Monitoring/Reporting/Review:
The IT Network Manager will ensure that full records are kept of:
➢ User Ids and requests for password changes
➢ User log-ons
➢ Security incidents related to this policy

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities:
The responsibility for the management of the school filtering policy will be held by the IT Network Manager. They will manage the school filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must
➢ be logged in change control logs within the filtering system
➢ be reported to a second responsible person, the IT Department Line Manager.

All users have a responsibility to report immediately to the ICT Team any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered. Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

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 broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. Ideally, 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.
➢ The school manages its own filtering service.
➢ The school has provided enhanced/differentiated user-level filtering through the use of the Netsweeper filtering programme allowing different filtering levels for different groups of users – staff/pupils/guest, etc.
➢ In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the IT Department Line Manager.
➢ Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems.
➢ Any filtering issues should be reported immediately to the filtering provider.
➢ Requests from staff for sites to be removed from the filtered list will be considered by the technical staff or Service Provider. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the online safety group.

Education/Training/Awareness:
Pupils will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:
➢ the Acceptable Use Agreement
➢ induction training
➢ staff meetings, briefings, training sessions

Parents/ carers will be informed of the school's filtering policy through the Acceptable Use Agreement and through online safety awareness sessions etc.

Changes to the Filtering System:
Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the ICT Team who will decide whether to make school level changes (as above).

Monitoring:

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the school online safety policy and the Acceptable Use Agreements. Monitoring will take place using NETSUPPORT DNA Safeguarding Software on all school devices utilising predefined government derived watch words.

Audit/Reporting:

Logs of filtering change controls and of filtering incidents will be made available to;

➢ ICT team
➢ Pastoral and Safeguarding teams
➢ online safety governor/governors committee
➢ external filtering provider/local authority/police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

Further Guidance:

➢ NEN Technical guidance: http://www.nen.gov.uk/advice/e-security-managing-and-maintaining-e-security-cyber-security-in-schools
➢ NEN –School e-Security Checklist
➢ Somerset Technical Guidance for schools – this checklist is particularly useful where a school uses external providers for its technical support/security:
➢ Prevent duty - 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" (Revised Prevent Duty Guidance: for England and Wales, 2015).
➢ Welsh Government - Respect and Resilience - Community Cohesion - Guidance and associated tool to support the development of community cohesion and prevent extremism in schools and other educational settings in Wales.
➢ In response to the above, the UK Safer Internet Centre produced guidance for schools on "Appropriate filtering and appropriate monitoring".

Appendix Six

Online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

BROWNEDGE ST MARY'S CATHOLIC HIGH SCHOOL

BROWNEDGE ST MARY'S CATHOLIC HIGH SCHOOL
'Let your light shine'

AI Policy

Approved by Full Governing Body	Date: December 2025

Signature of Head Teacher/Chair of Governors:	Date:

Policy amended by: N Oddie	Date: December 2025	Review Date: December 2027

Let Your Light Shine

If we love others, we live in the light. 1 John 2:10

Inspired by our Gospel Values, we have a shared responsibility to
- create an environment of welcome, love and respect for each member of our learning family.
- develop the unique gifts and talents of all, striving for excellence in everything we do.
- live out our commitment to love, service and justice in the local and global community.
- nurture the journey of faith and discovery for all
- celebrate and reflect on the love of God which is at the heart of all we are.

1. Aims

1.0 At Brownedge St Mary's, 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 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

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

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)](#)

3. Regulatory principles

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

Regulatory principle	WE WILL …
Safety, security and robustness	Ensure that AI solutions are secure and safe for users and protect users' data Ensure we can identify and rectify bias or error Anticipate threats such as hacking
Appropriate transparency and explainability	Be transparent about our use of AI, and make sure we understand the suggestions it makes
Fairness	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
Accountability and governance	Ensure that the governing board and staff have clear roles and responsibilities in relation to the monitoring, evaluation, maintenance and use of AI
Contestability and redress	Make sure that staff are empowered to correct and overrule AI suggestions – decisions should be made by the user of AI, not the technology Allow and respond appropriately to concerns and complaints where AI may have caused error resulting in adverse consequences or unfair treatment

4. Roles and responsibilities

4.0   AI Lead

Our generative AI lead is Mrs Oddie. They are responsible for the day-to-day leadership, ownership and management of AI use in the school.

4.1   Governing board

The governing board will:

> Take overall responsibility for monitoring this policy and holding the headteacher to account for its implementation in line with the school's AI strategy
> Ensure the headteacher is appropriately supported 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:
>> o Use AI tools responsibly and apply professional judgement when selecting AI tools for governance tasks, ensuring no identifiable pupil or staff data is entered into open AI platforms.
>> o Seek advice from the data protection officer / IT / AI lead and the designated safeguarding lead, as appropriate
>> o Check whether they are using an open or closed generative AI tool
>> o Ensure there is no identifiable information included in what they put into open generative AI tools
>> o Acknowledge or reference the use of generative AI in their work
>> o Fact-check results to make sure the information is accurate

4.2   Headteacher

The headteacher will:

> Take responsibility for the day-to-day leadership and management of AI use in the school
> Liaise with the data protection officer (DPO) 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
> Review and update this AI policy as appropriate, and at least every two years
> 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 new AI tools, taking into account advice from the DPO and data protection impact assessments

4.3   Data protection officer (DPO)

The data protection officer (DPO) is responsible for monitoring and advising on our compliance with data protection law, including in relation to the use of AI. Our DPO is Mr John Burrows

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 Miss Chloe Mellor

4.5   All staff

As part of our aim to reduce staff workload while improving outcomes for pupils, we encourage staff to explore opportunities to use AI tools in ways that support efficiency and enhance teaching and learning. Any use of AI must follow the guidelines set out in this policy.

To protect data and ensure responsible use, staff must:

- Use their professional judgement when selecting AI tools, ensuring that no identifiable pupil or staff data is entered into any platform
- Seek advice from the DPO or AI Lead where necessary
- Report safeguarding concerns to the DSL
- Understand whether the tool is open or closed, and apply appropriate caution
- Acknowledge or reference the use of generative AI where appropriate
- Fact-check outputs for accuracy, bias and suitability
- Use the appendix checklist to support decision-making where helpful

All staff play a role in helping pupils understand both the benefits and limitations of AI and in developing pupils' ability to critically evaluate AI-generated content.

4.6 Pupils

Pupils must follow the guidelines set out in section 7 of this policy ('Use of AI by pupils')

5. Staff and governors' use of AI

5.1   Use of AI

We are committed to helping staff and governors reduce workload and enhance professional practice through the responsible use of AI. Staff may use AI tools at their professional discretion to support planning, teaching, assessment and administration, provided no identifiable pupil or staff data is entered and all outputs are checked for accuracy, bias and appropriateness.

Where helpful, staff are encouraged to use the checklist in Appendix One to support decision-making. AI can accelerate certain tasks, but it must never replace professional judgement or the expertise required for teaching, assessment or pastoral care.

The quality and accuracy of any work produced with AI remains the responsibility of the individual who uses it. AI-generated content used for planning or resource creation should be clearly attributed where appropriate and only shared with colleagues once reviewed for accuracy.

Always consider whether AI is the right tool for the task; its availability does not mean it is always appropriate.

5.2   Process for approval

Staff are welcome to suggest new ways of using AI with pupils to improve outcomes or support learning. Such proposals should be discussed with the headteacher, who is responsible for approving any AI tools or uses involving pupils, taking into account safeguarding, data protection advice and relevant risk assessments.

5.3   Data protection and privacy

To ensure that personal and sensitive data remains secure, no one will be 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, Brownedge St Mary's will treat this as a data breach and will follow the personal data breach procedure outlined in our data protection policy.

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.

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 ensure we can identify and rectify bias or error by training staff in this area.

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

If parents/carers 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 usual complaints' procedure.

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's child protection and safeguarding policy.

5.7   Ethical and responsible use

We will always:

- Use generative AI tools ethically and responsibly
- Remember the principles set out in our school's equality policy when using generative AI tools
- 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

6. Educating pupils about AI

Here at Brownedge St Mary's, 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.

In KS3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in KS4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the end of secondary school, pupils will know:

- Rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- Online risks, including the importance of being cautious about sharing personal information online and of using privacy and location settings appropriately to protect information online. Pupils should also understand the difference between public and private online spaces and related safety issues
- The characteristics of social media, including that some social media accounts are fake, and / or may post things which aren't real / have been created with AI. That social media users may say things in more extreme ways than they might in face-to-face situations, and that some users present highly exaggerated or idealised profiles of themselves online
- Not to provide material to others that they would not want to be distributed further and not to pass on personal material which is sent to them. Pupils should understand that any material provided online might be circulated, and that once this has happened there is no way of controlling where it ends up. Pupils should understand the serious risks of sending material to others, including the law concerning the sharing of images
- That keeping or forwarding indecent or sexual images of someone under 18 is a crime, even if the photo is of themselves or of someone who has consented, and even if the image was created by the child and/or using AI-generated imagery. Pupils should understand the potentially serious consequences of acquiring or generating indecent or sexual images of someone under 18, including the potential for criminal charges and severe penalties including imprisonment. Pupils should know how to seek support and should understand that they will not be in trouble for asking for help, either at school or with the police, if an image of themselves has been shared. Pupils should also understand that sharing indecent images of people over 18 without consent is a crime
- What to do and how to report when they are concerned about material that has been circulated, including personal information, images or videos, and how to manage issues online
- About the prevalence of deepfakes including videos and photos, how deepfakes can be used maliciously as well as for entertainment, the harms that can be caused by deepfakes and how to identify them
- That social media can lead to escalations in conflicts, how to avoid these escalations and where to go for help and advice
- How to identify when technology and social media is used as part of bullying, harassment, stalking, coercive and controlling behaviour, and other forms of abusive and/or illegal behaviour and how to seek support about concerns
- How information and data is generated, collected, shared and used online
- That websites may share personal data about their users, and information collected on their internet use, for commercial purposes (e.g. to enable targeted advertising)
- That AI chatbots are an example of how AI is rapidly developing, and that these can pose risks by creating fake intimacy or offering harmful advice. It is important to be able to critically think about new types of technology as they appear online and how they might pose a risk

7. Use of AI by pupils

We recognise that AI can help pupils learn when used safely and appropriately. Pupils may use AI functions built into search engines (such as Google's AI-supported search mode) for supervised research. AI may also be used during specific learning activities, such as computing tasks or art projects involving AI-generated images.

However, many AI tools require age verification or parental consent and cannot be universally restricted across all platforms. Pupils must therefore understand clearly what is and is not permitted in school and take responsibility for following these expectations.

To maintain academic integrity, pupils may not use AI tools:

- During internal or external assessments
- To generate homework or classwork that is submitted as their own
- To produce answers, explanations or solutions without teacher guidance

Any unreferenced use of AI is considered plagiarism. When AI is used as a research source, pupils must reference the tool and date of generation.

Pupils must never use AI to generate harmful, offensive, discriminatory or inappropriate content, including impersonation, harassment or inappropriate images.

7.1   Formal assessments

We will continue to take reasonable steps where applicable to prevent malpractice involving the use of generative AI in assessments.

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

8. Use of AI by staff

AI tools are permitted for staff use and can support tasks such as lesson planning, resource creation, anonymised administrative drafting, brainstorming and idea development. Their use should enhance efficiency, creativity and teaching practice, while remaining aligned with the school's educational values. AI must never replace human interaction or professional judgement in matters requiring staff expertise or care.

Staff may use AI tools at their professional discretion, provided no identifiable pupil or staff data is entered and all outputs are checked for accuracy, bias and appropriateness. Human oversight must remain central at all times. Any AI tool used directly by pupils, or incorporated into pupil activities, must be approved by the school.

Closed generative AI tools provide greater security and data protection because they operate within protected environments rather than storing or learning from user inputs. Open tools may store data, learn from prompts or process information outside the UK. For this reason, the school strongly encourages the use of closed generative AI wherever possible, particularly when working with curriculum materials, internal documents or content that could identify individuals. We advise all members of staff to ensure that settings on "Open" generative platforms are set to not share your data to train any models. This means, for example in ChatGPT, turning the "model improvement for everyone" setting to OFF.

At present, Microsoft Copilot offers the most secure environment for staff use. Open tools such as ChatGPT and Google Gemini may also be used with caution, following a clear risk assessment to ensure safeguarding, data protection and filtering requirements are met.

AI must never be used to:

- Make or influence pupil assessment grades
- Draft or submit safeguarding concerns or referrals
- Write staff performance appraisals or confidential HR reports

These tasks require human oversight and professional judgement.

9. Staff training

We are committed to ensuring that all staff develop a confident, informed, and responsible understanding of AI as it evolves. To support this, AI awareness and safe practice will be embedded within the school's wider programme of digital literacy and online safety training. Annual safeguarding and safe internet-use training will include specific guidance on the opportunities and risks associated with AI, including data protection, bias, misinformation, and the responsible use of generative tools.

Ongoing professional development will be coordinated by the SLT in collaboration with the AI Working Party and CPD Lead. They will ensure staff have regular access to high-quality CPD opportunities—both internal and external—including briefings, workshops, online modules, and subject-specific development sessions. These opportunities will be reviewed annually to ensure they reflect current best practice and emerging technologies.

The school will remain up to date with national guidance, research, and sector-wide developments by engaging with recognised educational bodies, professional networks, and local authority or trust-led digital learning groups. Good practice will be shared through termly staff meetings, and peer-led training, ensuring new insights and strategies are accessible across departments. Staff will be encouraged to trial AI tools within a safe, ethical framework and to share reflections to support continuous improvement and collective professional growth.

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 according to the procedures set out in the school's child protection and safeguarding policy.

11. Breach of this policy

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.

11.2 By pupils

Any breach of this policy by a pupil will be dealt with in line with our behaviour policy.

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 the Headteacher 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 regularly reviewed and updated to align with emerging best practices, technological advancements and changes in regulations.

The policy will be shared with the full governing board at least every two years.

All teaching staff are expected to read and follow this policy. The Headteacher is responsible for ensuring that the policy is followed and 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/carers and staff will be considered in the ongoing evaluation and development of AI use in school.

13. Links with other policies

This AI policy is linked to our:

- › Data protection policy
- › Safeguarding/child protection policy
- › Teaching and Learning policy including Homework Policy
- › Behaviour policy
- › Staff code of conduct
- › Pupil, Staff and Governors Acceptable Use Policy
- › Online safety policy
- › Equality policy

AI Use Checklist for Staff

Use this checklist each time you choose an AI tool to support your work.

1. Purpose

□ I have a clear educational or workload-reduction purpose for using AI.
□ AI is the right tool for this specific task.

2. Data Protection

□ I am not entering any personal, sensitive, or identifiable pupil data.
□ I am not entering sensitive staff information.
□ I understand whether the tool is "open" or "closed".

3. Accuracy & Professional Oversight

□ I will check the AI output for accuracy, bias, and appropriateness.
□ I remain fully responsible for the final content.
□ I am willing to acknowledge that AI assisted this work if shared.

4. Ethics & Safeguarding

□ The AI use is safe, ethical, and aligns with safeguarding expectations.
□ The task does **not** involve assessment judgments, safeguarding reports, or HR matters.
□ The tool cannot accidentally generate harmful or inappropriate content.

5. Compliance with School Policy

□ My use aligns with school AI policy and GDPR responsibilities.
□ If pupils will use the tool, it **is school-approved** and age-appropriate.

6. Impact on Learning

□ This use of AI enhances learning, support, or efficiency.
□ It does not reduce pupil independence, thinking, or skill development.

🟢 **If all boxes are ticked → It is appropriate to use the AI tool.**
🔴 **If any box is NOT ticked → Reconsider or seek advice before using AI.**