

St Matthew's High Brooms CE Primary School

Powder Mill Lane
Tunbridge Wells
Kent
TN4 9DY



Online Safety Policy

Headteacher: Claire Harris
Chair of Governors: Sarah Warshow

Ratified: July 2026
Next Review: July 2027

Fulfilling God-given potential

*Distinctive Christian values-
Honesty, Kindness, Respect, Responsibility*

Contents

1. Aims
2. Legislation and Guidance
3. Roles and responsibilities
4. Educating pupils about online safety
5. Educating parents about online safety
6. Cyber-bullying
7. Acceptable use of the internet in school
8. Pupils using mobile devices in school
9. Staff using work devices outside school
10. How the school will respond to issues of misuse
11. Training
12. Monitoring arrangements
13. Links with other policies

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- 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, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

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

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

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

The policy also considers 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, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure 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 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 their safeguarding needs.

The governor who oversees online safety is the Safeguarding Link Governor.

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 3)
- 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.

3.3 The designated safeguarding lead

Details of the school's DSL and deputies 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 annually 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
- Working with the ICT technician to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT technician and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged 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
- Undertaking annual risk assessments that consider and reflect the risks children face
- 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

This list is not intended to be exhaustive.

3.4 The ICT technician

The ICT technician is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure 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 monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 1) 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

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use: see Acceptable Use Policy: <https://st-matthews-school.org/our-school/policies>
- 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 by email to DSL/ICT technician
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 1) 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

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

- What are the issues? - [UK Safer Internet Centre](#)
- Hot topics - [Childnet International](#)
- Parent factsheet - [Childnet International](#)
- Healthy relationships – [Disrespect Nobody](#)
- School Website: <https://st-matthews-school.org/parents/e-safety>

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.

4. Educating pupils about online safety

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

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Be discerning in evaluating digital content

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

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- Where and how to report concerns and get support with issues online

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

St Matthew's recognise that some children may need a more personalised or contextualised approach, tailored to the specific needs and vulnerabilities of individual children, for example children who are victims of abuse, neglect or exploitation, and children with SEND.

5. Educating parents about online safety

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

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the class teacher who may refer the parent to the headteacher and/or the DSL.

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

6. Cyber-bullying

6.1 Definition

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

Class teachers 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 personal, social, health and economic (PSHE) education, and other subjects where appropriate.

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

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

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

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will 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 by the headteacher 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 / DSL
- 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 or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- 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 headteacher in consultation with DSL 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:

- **Not** view the image
- 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 [screening, searching and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

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

6.4 Artificial intelligence (AI)

Understanding AI in Education

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT, Google Gemini (formerly Bard), Microsoft Copilot, and image generation tools such as DALL-E and Midjourney.

St Matthew's recognises that AI has significant potential to:

- Support pupils' learning and creativity
- Assist with research and information gathering
- Help develop digital literacy skills
- Provide personalised learning experiences

However, we also recognise the risks and challenges associated with AI use in education.

Risks Associated with AI

AI tools may present the following risks to pupils:

1. Bullying and Harmful Content

- **Deepfakes:** AI can be used to create realistic but fake images, audio or video content that appears to show someone doing or saying things they never did
- **Deepfake pornography:** Pornographic content created using AI to include someone's likeness without their consent
- **Impersonation:** Creating fake social media profiles or messages that appear to be from someone else
- **Manipulation of images:** Altering photographs to embarrass, humiliate or harm others

2. Academic Integrity

- Pupils using AI to complete homework or assessments without proper attribution
- Over-reliance on AI tools preventing development of critical thinking skills
- Plagiarism concerns when AI-generated content is presented as original work

3. Privacy and Data Protection

- Pupils sharing personal or sensitive information with AI tools
- Data being stored or used by AI companies in ways pupils don't understand
- Lack of understanding about how AI tools collect and use data

4. Misinformation and Bias

- AI tools can produce inaccurate or misleading information presented as fact
- AI systems may reflect biases in their training data
- Pupils may not critically evaluate AI-generated content

5. Age-Inappropriate Content

- Some AI tools are not designed for children and may produce inappropriate responses
- Lack of effective content filtering on some AI platforms

Our Approach to AI

Teaching About AI

St Matthew's will ensure pupils receive age-appropriate education about AI, including:

Key Stage 1:

- Basic understanding that computers and technology can help us learn
- Awareness that not everything online is real or true
- Understanding that they should always ask a trusted adult before using new technology

Key Stage 2:

- Understanding what AI is and how it works in simple terms
- Recognising that AI tools can make mistakes and produce false information
- Learning to question and verify information from any source, including AI
- Understanding the importance of not sharing personal information with AI tools
- Recognising that using AI to complete work without acknowledgment is dishonest
- Understanding that images and videos can be manipulated or created artificially
- Knowing how to report concerns about AI-generated content

This teaching will be integrated into:

- Computing lessons
- PSHE education
- Online safety sessions
- Relevant curriculum subjects where AI is discussed

Staff Use of AI

Staff may use AI tools to support their professional work, including:

- Lesson planning and resource creation
- Administrative tasks
- Professional development

When using AI tools, staff must:

- Conduct a risk assessment before introducing new AI tools to pupils
- Ensure any AI tools used with pupils are age-appropriate and have appropriate safety features
- Not input any personal, sensitive or confidential information about pupils, staff or families into AI tools
- Comply with data protection requirements and the school's Data Protection Policy
- Model critical evaluation of AI-generated content
- Be transparent with pupils about when and how AI is being used
- Ensure that any AI-generated content used in teaching is checked for accuracy and appropriateness
- Consider accessibility needs when using AI tools

Pupil Use of AI

Pupils may use AI tools in school under the following conditions:

- Only with explicit permission and supervision from a teacher
- Only using school-approved AI tools that have been risk-assessed
- With clear guidance on appropriate and inappropriate uses
- With understanding of how to use AI responsibly and ethically

When pupils use AI tools, they must:

- Always acknowledge when AI has been used to support their work
- Check AI-generated information for accuracy
- Not share personal information with AI tools
- Report any concerning or inappropriate content generated by AI
- Use AI to support learning, not replace their own thinking and effort

Responding to AI-Related Incidents

St Matthew's will treat any use of AI to bully, harm or deceive others seriously. This includes:

Bullying and Harmful Content:

- Any use of AI to create deepfakes, manipulated images, or fake content about pupils or staff will be dealt with in line with our Anti-Bullying Policy and Behaviour Policy
- Incidents involving deepfake pornography or other illegal content will be reported to the police
- The DSL will be informed immediately of any incidents involving AI-generated harmful content

Academic Misconduct:

- Pupils who use AI inappropriately to complete work will face consequences in line with the school's Behaviour Policy
- Teachers will work with pupils to help them understand appropriate use of AI as a learning tool

Safeguarding Concerns:

- Any AI-related incident that raises safeguarding concerns will be handled in line with the school's Child Protection and Safeguarding Policy
- The DSL will assess whether external agencies need to be involved

Reporting AI-Related Concerns

Pupils should report concerns about AI to:

- Their class teacher
- Any trusted adult in school

Staff should report concerns about AI to:

- The DSL: Carolyn Pollard
- The ICT technician: Simon Witherington
- The Headteacher

Parents/carers should report concerns to:

- The class teacher
- The DSL: Carolyn Pollard
- The Headteacher

Supporting Parents/Carers

The school will support parents/carers to understand AI risks and opportunities through:

- Information on the school website
- Parent workshops or information sessions
- Letters or communications home when relevant
- Signposting to reliable resources about AI and online safety

Useful Resources for Parents:

- [Include links to relevant resources such as Internet Matters, NSPCC, UK Safer Internet Centre]

Monitoring and Review

Given the rapidly evolving nature of AI technology:

- The DSL and ICT technician will monitor developments in AI and update this policy as needed
- Staff will receive regular updates on AI-related risks and appropriate responses
- The school will review AI-related incidents to identify patterns and inform future practice
- This section will be reviewed at least annually, or more frequently if significant developments occur

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. 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.

More information is set out in the Acceptable Use policy.

Use of AI tools:

Any use of AI tools in school must:

- Be approved by the DSL and ICT technician
- Have a completed risk assessment
- Be supervised by staff
- Comply with data protection requirements
- Be age-appropriate
- Support educational objectives

Pupils must not use AI tools to:

- Create deepfakes or manipulated images
- Complete assessed work without acknowledgement
- Share personal or sensitive information
- Bully or harm others
- Access inappropriate content

8. Pupils using mobile devices in school

Pupils who wish to bring mobile devices into school must have a permission slip signed by their parents and agreed by the school. They are not permitted to use them on the school site and during:

- Lessons
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the Acceptable Use Policy and Image Use Policy.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use policy.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice the ICT technician.

10. 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 policies on behaviour and acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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

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

11. Training

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

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

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

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, harassing, and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element
- There are risks and opportunities presented by AI in education
- How to identify and respond to AI-related safeguarding concerns
- How to teach pupils about AI safely and effectively
- How to complete risk assessments for AI tools
- The school's policies on AI use
- How to identify AI-generated content, including deepfakes

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
- Understand their roles and responsibilities for online safety eg; filtering and monitoring in school, age appropriate lesson planning.

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

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

Volunteers will receive appropriate training and updates, if applicable.

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

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. CPOMs is used for logging incidents involving pupils. An incident involving staff would be logged as a low-level concern initially, which the Headteacher would review in line with Staff disciplinary procedures.

This policy will be reviewed annually by the DSL. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Acceptable Use policy
- Image Use Policy