



Contents

1. Introduction	1
2. Aims	1
3. Legislation and guidance	2
4. Roles and responsibilities	2
5. Educating students about online safety and digital conduct	5
6. Educating parents/carers about online safety	6
7. Cyber-bullying	7
8. Examining electronic devices	7
9. Acceptable use of internet in school	8
10. Staff using work devices outside school	8
11. Training for staff, trustees and volunteers	8
12. Student use of mobile phones (and other devices) in school	9
13. Student use of school devices	11
14. Artificial Intelligence (AI)	11

1. Introduction

This policy supersedes and replaces the school's previous Online Safety Policy, incorporates the Student Use of Mobile Phones Policy, introduces new sections on the safe and responsible use of artificial intelligence (AI), and includes revised Online Safety Acceptable Use Agreements for all stakeholders.

Beaumont School recognises that internet, mobile and digital technologies provide powerful opportunities for students to learn, connect and thrive. At the same time, we acknowledge the challenges and risks that the fast-moving digital world presents. A student's future success may, in part, depend on their digital skills, their use of emerging technologies such as artificial intelligence (AI), and their online reputation. We are committed to preparing them to use technology safely, responsibly and respectfully.

Online safety and digital conduct form an essential part of our safeguarding responsibilities. All students, staff and trustees will be supported to develop the knowledge, skills and behaviours needed to navigate the digital environment confidently. We recognise that some students may require additional teaching, reminders or tailored support to reinforce their understanding of digital safety.

We are equally committed to ensuring that all members of our community, including parents and carers, are informed about the evolving digital landscape — from social media and mobile devices to AI-powered tools — so that they can play an active role in helping children make safe and positive choices online.

This policy is designed to protect the interests and safety of the entire Beaumont community. It should be read alongside related policies and procedures, including Child Protection, GDPR, Health and Safety, Behaviour, Anti-Bullying and the Staff Code of Conduct.

2. Aims

Beaumont School aims to:

- Have robust processes in place to ensure the online and digital safety and security of students, staff, volunteers and trustees.
- Identify and support groups of students that are potentially at greater risk of harm online than others.

- Deliver an effective approach to online safety and digital conduct which empowers us to protect and educate the whole school community in its use of technology, including personal devices, mobile phones, school-issued devices, and emerging technologies such as artificial intelligence (AI).
- Promote the safe, responsible and ethical use of AI by ensuring students and staff understand its capabilities and limitations, use it within a clear framework that protects the integrity of student work and academic honesty, safeguard personal and school data, remain alert to potential harms, and develop the confidence to use AI appropriately to enhance study, work and life beyond school.
- Establish clear mechanisms to identify, intervene and escalate incidents where appropriate.

The 4 key categories of risk

Our approach to online safety and digital conduct is based on addressing the following categories of risk outlined in Keeping Children Safe in Education (KCSIE):

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including AI-generated deepfakes and 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 people with the intention to groom or exploit the user.

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images, sharing explicit images, misuse of AI, and online bullying.

Commerce – risks such as online gambling, inappropriate advertising, phishing, sextortion and/or financial scams, including those that may exploit AI.

3. 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 in schools](#)
- [Preventing 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 students' electronic devices where they believe there is a 'good reason' to do so.

The section on Artificial Intelligence (AI) 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)

It 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 \(DPA 2018\)](#)

This policy complies with our funding agreement and articles of association.

4. Roles and responsibilities

4.1 Board of Trustees

The Board of Trustees has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

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

The Board of Trustees 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 Board of Trustees will make sure that the school teaches students how to keep themselves and others safe, including online.

The Board of Trustees 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 Trustees who oversee online safety are Gill Shearsby-Fox and Liz Spooner.

All trustees will:

- Make sure 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)
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures

4.2 The Headteacher

The Headteacher is responsible for making sure that staff understand this policy, and that it is implemented consistently throughout the school.

4.3 Online Safety Lead and Co-Lead

The Online Safety Lead is the Designated Safeguarding Lead, Danielle Irving (Assistant Headteacher), working with Andy Gray (Assistant Headteacher) as Online Safety Co-Lead. All breaches of this policy must be reported to Danielle Irving or Andy Gray. Their work is supported by the school's Deputy Designated Safeguarding Leads (DDSLs), as set out in our child protection policy, and other members of the pastoral team where appropriate.

The Online Safety Leads take responsibility for online safety in school, in particular:

- Supporting the Headteacher in making sure that staff understand this policy and that it is implemented consistently throughout the school
- Working with the Headteacher and Board of Trustees to review this policy annually and make sure 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 trustees with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the Network Manager to make sure the appropriate systems and processes are in place
- Working with the Headteacher, Network 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
- Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Making sure 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
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and/or Board of Trustees via the link trustee for Online Safety
- Undertaking regular training that considers the risks students 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
- Being aware of new and emerging safeguarding threats posed by AI
- Updating and delivering staff training on AI safeguarding threats

This list is not intended to be exhaustive.

4.4 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 make sure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Making sure 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
- Making sure that any online safety incidents are passed in line with this policy

This list is not intended to be exhaustive.

4.5 Data, Assessment and Monitoring Officer

The Data, Assessment and Monitoring Officer is responsible for:

- The day-to-day oversight of the school's filtering and monitoring software, reviewing system alerts and reports on student activity
- Flagging safeguarding-related concerns to the Designated Safeguarding Lead (or Deputy) without delay
- Passing on behaviour-related concerns to the relevant teacher, pastoral lead or Head of Year, in line with the Behaviour Policy
- Ensuring that a log of concerns is maintained and shared appropriately

4.6 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 Brenda Austin and is contactable via dpo@beaumont.school.

4.7 All staff and volunteers

All staff, including contractors, 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, AI and the internet (Appendix 3), and making sure that students follow the school's terms on acceptable use (Appendices 1 and 2)
- 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 immediately alerting the Online Safety Leads and the Network Manager
- Following the correct procedures by speaking with the Online Safety Leads and Network Manager if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to make sure that any online safety incidents are logged 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
- 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'

- Making sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students 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

This list is not intended to be exhaustive.

4.8 Parents and carers

Parents/carers are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Make sure that their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (Appendices 1 and 2)
- Seek further guidance, as required, on keeping children safe online from the relevant sections of the Beaumont website, which includes links to other following organisations and websites including the UK Safer Internet Centre.

4.9 Visitors

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

5. Educating students about online safety and digital conduct

Students will be taught about online safety and digital conduct as part of the curriculum, primarily as part of the Life Skills (PSHCEE) curriculum in accordance with the statutory [Relationships and sex education \(RSE\) and health education](#) guidance for schools. The safe use of social media and the internet (including generative AI) will also be covered in other areas of school (e.g. tutor time and assemblies) and in other subjects where relevant (e.g. Computer Science). Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable students, victims of abuse and some students with SEND. Although this guidance does not extend to Key Stage 5, the school will continue to provide age-appropriate education on online safety, digital conduct and the responsible use of technology to students in the Sixth Form.

As outlined in the statutory guidance, in **KS3**, students 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

Students 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**, students 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. Students 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. Students 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. Students 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. Students 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. Students 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. Students 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. Students should be taught where to go for advice and support about something they have seen online. Students 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 students 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

In addition to meeting statutory requirements, Beaumont goes further by embedding online safety and digital conduct across the wider curriculum, including the pastoral curriculum, addressing emerging issues such as AI, digital wellbeing, misinformation, and academic integrity, and ensuring students are prepared to use technology responsibly in all aspects of their lives.

Students will receive age-appropriate training on safe internet use, including password security and safeguarding issues, such as cyberbullying and online radicalisation.

6. Educating parents/carers about online safety

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

Online safety will also be covered during parent information evenings at the start of each academic year for all year groups.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use:
 - Filtering: RM SafetyNet - HFL Broadband
 - Monitoring: Classroom.cloud
- What their children are being asked to do online, including the sites they will be regularly asked to access and who from the school (if anyone) their child will be interacting with online

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

Concerns or queries about this policy can be raised with the Online Safety Lead or a member of the safeguarding team.

7. Cyber-bullying

7.1 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 a person or group by another person or group, where the relationship involves an imbalance of power. (See also the School Behaviour Policy.)

7.2 Preventing and addressing cyber-bullying

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

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their classes in accordance with our Life Skills curriculum.

Staff receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

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 Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among students, 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.

8. Examining electronic devices

The Headteacher, and any member of staff authorised to do so by the Headteacher (as set out in our Behaviour Policy), can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or students, 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 students and staff. If the search is not urgent, they will seek advice from the DSL, Deputy, or a member of the Senior Leadership Team
- Explain to the student why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- Seek the student'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 will need to consider whether there are reasonable grounds for suspecting that the device 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 the DSL (or Deputy) 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 whether 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 student 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 Deputy) 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 students 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 students' electronic devices will be dealt with through the School Complaints Procedure.

9. Acceptable use of internet in school

All students, parents/carers, staff, volunteers and trustees 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 students, staff, volunteers, trustees 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.

10. 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 in line with the school's password requirement
- Making sure the device is locked if left unsupervised
- Not sharing the device among family or friends
- Keeping operating systems up to date by promptly installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in Appendix 3.

Staff members must only use a school-issued device primarily for business use; all other uses are secondary and must not interfere with my work duties or breach any other school policies. Only "insignificant" personal use is permitted, examples of which might include checking personal email or online banking.

If staff have any concerns over the security of their device, they must seek advice from the Network Manager in the first instance.

11. Training for staff, trustees and volunteers

Staff will receive training 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 are capable of abusing 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, which 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 students can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and 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.

Trustees 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 Policy.

12. Student use of mobile phones (and other devices) in school

At Beaumont School we recognise that mobile phones, including smart phones, and associated devices (such as tablets, smartwatches and smart glasses), are an important part of everyday life for many of our students, staff and the wider school community. Despite this, we also know that these devices can risk unnecessary distraction, disruption and diversion. At all times, we aim to maintain a positive and safe learning environment for our students, so they all, whatever their background, can enjoy and excel.

For the purposes of this policy, smartwatches and other wearable smart devices are treated in the same way as mobile phones. If a smartwatch is seen, heard or used in contravention of this policy, it will be confiscated in line with the school Behaviour Policy. Basic digital watches without communication or internet-enabled functionality are permitted.

Beaumont is transitioning toward becoming a fully smartphone-free environment. Effective September 2026, a complete ban on smartphones will be formalised for all students entering Year 7 for the duration of their time at Beaumont up to and including Year 11. This policy will operate on a rolling basis. The smartphone ban will extend to each subsequent new Year 7 cohort as they join the school, eventually covering all year groups up to and including Year 11.

12.1 Students in Year 7 (from September 2026)

Effective from September 2026, smartphones are classified as prohibited items for all students in Year 7. Students in this year group are strictly prohibited from bringing smartphones onto the school premises at any time. Year 7 students may bring a basic non-smartphone (commonly referred to as a 'feature phone' or 'brick phone') that is limited to calling and texting only, without internet browsing or social media capabilities. These devices must be switched off at all times during the school day. They must be stored securely either in the student's locker or at the bottom of their school bag. Devices must not be kept in blazer pockets or clothing. Any smartphone brought to school by a Year 7 student, or any

non-smartphone that is visible, used, or turned on during the school day, will be immediately confiscated in accordance with the school Behaviour Policy.

12.2 Students in Years 8-11 (from September 2026)

Students at Beaumont are allowed to bring a mobile phone to school if they wish to do so. There is no expectation for students to bring a mobile phone, but we recognise that many choose to do so e.g. those that are travelling to and from school by themselves.

12.3 Student Use of Mobile Phones and Devices in Years 7-11

Students are allowed to keep personal possession of their mobile phones only on the strict condition that they are never used, seen or heard in school. This condition also applies to associated devices such as tablets, smartwatches and smart glasses. This rule applies from the point that students enter the school site to the point where they leave the school site. If a student is seen or found in contravention of this rule, the device(s) will be confiscated in line with our behaviour policy. Students bringing mobile phones and/or associated devices to school must ensure that they are stored appropriately during the school day so that they comply with the rules set out in the behaviour policy.

This rule applies to all parts of the school day, including lesson and curriculum time. Teachers must not ask students in Years 7-11 to use a mobile phone in a lesson. If it is determined that access to a device would be beneficial to support learning, teachers must plan for this and arrange for a school-issued device to be used e.g. arranging to use a Chromebook trolley or booking a PC room. There are no exceptions to this rule during the school day while students are on site.

12.4 Students in Sixth Form

Students in the Sixth Form are permitted to bring a mobile phone, including a smart phone, to school.

Sixth Form students are permitted to use a mobile phone in designated areas of the school only. These areas are:

- Sixth Form common room
- Sixth Form atrium
- Covered area outside the Sixth Form area

Outside of these areas, Sixth Form students must also ensure that their phones are never used, seen or heard in school.

However, teachers and form tutors are permitted to direct students in Sixth Form to use a mobile phone in a lesson to support student learning. Students are only permitted to use their phone with the direct permission of the teacher and for the specific task(s) they are asked to complete. Where this is done, teachers are responsible for actively monitoring the use of mobile phones (e.g. by circulating the classroom or observing students from the back of the classroom).

12.5 Use of mobile phones by students on day trips

Whilst on day trips, students must follow the school's rules on mobile phones set out in this policy above.

Students are permitted to use mobile phones to communicate with parents/carers about finish times and collection arrangements before and after day trips, but only with express permission of the supervising member(s) of staff. Otherwise mobile phones must not be used, seen or heard.

12.6 Use of mobile phones by students on residential trips

Mobile phones are not permitted on KS3 residential trips during term-time.

For other residential trips, our default position is that students must follow the school's rules on mobile phones set out in this policy. However, acceptable phone usage will be communicated via trip information evenings prior to departure, which could make exceptions based on the nature of the trip (e.g. itinerary and age group). Any adaptations to the default position will be agreed by the Assistant Headteacher with responsibility for Trips and Visits.

12.7 Use of mobile phones by students off-site for PE fixtures, tournaments and events

Whilst representing the school at a sporting fixture or event, students must follow the school's rules and regulations on mobile phones as set out in this policy.

Students are permitted to use mobile phones to communicate with parents/carers about finish times and collection arrangements before and after fixtures but only with express permission of the supervising member(s) of staff. Otherwise mobile phones must not be used, seen or heard.

12.8 Consequences of mobile phone misuse

Schools are permitted to confiscate phones from students under sections 91 and 94 of the Education and Inspections Act 2006.

If a student is seen or found to be in contravention of the rules set out in this policy, the device(s) will be confiscated in line with the school's Behaviour Policy. This covers the specific consequences, retention periods, and retrieval procedures for any confiscated devices.

The use of mobile phones or associated devices to photograph, film, record or share images, audio or video of students or staff without permission is strictly prohibited and will be treated as a serious behaviour and safeguarding matter.

The misuse of mobile phones or associated devices may also result in further sanctions where appropriate, including where devices are used for:

- bullying, harassment or intimidation
- inappropriate use of social media
- sharing inappropriate or offensive material
- accessing or generating inappropriate content using artificial intelligence (AI) tools
- cheating or malpractice in assessments or examinations

In serious cases, the school may involve external agencies, including the police, in accordance with safeguarding procedures and statutory guidance.

12.9 Exemption for significant medical need

Students with diagnosed significant medical needs, such as diabetes, are permitted to carry and use a mobile phone during school hours if this is required to effectively manage their medical conditions, particularly in emergency situations. To qualify for this exemption, parents/carers must provide the school with medical documentation from a healthcare professional confirming the student's condition and the necessity for mobile phone use. This requirement must also be part of the student's Individual Health Plan (IHP). The phone should be used solely for medical purposes, and students are expected to adhere to all other aspects of the school's rules and regulations on mobile phones as set out in this policy.

12.10 Loss, Theft and Damage

The school accepts no responsibility for the loss, theft or damage of mobile phones or associated devices brought onto the school site. Confiscated devices will be stored securely in accordance with school procedures until they are returned in line with the Behaviour Policy.

13. Student use of school devices

School-issued devices, including Chromebooks—such as those provided under the Year 7 1:1 Device Scheme (launching September 2026) - are provided to support and enhance student learning. This policy applies to all students allocated or using a school-managed device, including:

- Participants in the **Year 7 1:1 Device Scheme** (commencing September 2026)
- Students in older year groups who have been allocated or loaned a school-covered or school-managed Chromebook.
- Students using a school-owned device such as a computer in a PC suite

All students must adhere to the rules outlined in the AUA.

14. Artificial Intelligence (AI)

The purpose of this section of the policy is to set clear guidelines for how staff and students can harness the opportunities of generative artificial intelligence (AI) but do so in a way that ensures the technology is used in an

effective, safe and policy-compliant manner. Generative AI tools are now widespread and easy to access. Staff, students and parents/carers are likely to be familiar with generative chatbots such as ChatGPT and Google Gemini.

14.1 Definition

For the purposes of this policy, 'Generative Artificial Intelligence' or 'AI' refers to any tool in which the model generates new content on behalf of the user. This content could take the form of text, image, audio, video or computing code, although this is not an exhaustive list. Examples of AI tools include Large Language Models (LLMs) such as ChatGPT, Google Gemini, Claude and Perplexity, and image generation tools such as Dall-E3 and Midjourney. The definition also extends to any software which includes 'built-in' elements of generative artificial intelligence such as Microsoft Co-Pilot and Canva.

14.2 Key Principles

Our whole-school approach to AI is underpinned by the following six key principles:

1. **Developing understanding** - to ensure that staff, students and parents/carers are aware of the capabilities, limitations and potential impact of AI so that it is used appropriately, and in line with the guidelines set out in this policy.
2. **Maintaining integrity and authenticity of student work** - to ensure that any use of AI is done within an acceptable, clearly-defined framework so that any work submitted for classwork, home learning and formal assessment (including NEA) is the student's own or, where permitted, is correctly referenced.
3. **Detecting and deterring malpractice** - to ensure that staff are supported in detecting and deterring possible malpractice through the use of AI to maintain the academic integrity of our curriculum and assessment practice.
4. **Protecting our data** - to ensure that staff and students are aware of their obligations to protect data when using generative AI tools in accordance with data protection legislation and Beaumont's existing Data Privacy and Online Acceptable Usage Policies.
5. **Safeguarding** - to ensure that we keep our students safe from the possible harms of generative AI by educating them on the topic and fulfilling our obligations to prevent them from accessing or creating harmful or inappropriate content online.
6. **Future-proofing** - to ensure that our staff and students are well-informed and confident users of emerging technologies, including generative AI, and are empowered to use them responsibly to take full advantage of the opportunities they provide for both work and study.

14.3 Acceptable usage of artificial intelligence (AI) for staff

Our approach for staff use of AI is guided by the principles outlined in section 9.2. For staff members, these are complemented by our commitment to the following:



Staff are welcome to use approved AI tools to support and improve their professional practice, on the understanding that they are responsible for the output and use of the output of these tools.

Output from AI tools must, on every occasion, be reviewed before use, especially when the output is directed to students, parents/carers and other interested parties.

Staff must comply with the school's ICT AUA and data protection principles. All staff are aware that any text entered into an AI tool is potentially being made public. If staff are using AI for any professional reason, personal or sensitive data regarding students, staff or the school must not be entered.

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 individuals who may be affected by them, including, but not limited to, students and staff.

The use of new AI tools requires approval from the Online Safety Leads.

14.4 Intellectual property

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

Students 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.

Examples of what may be deemed original creative work include:

- Essays, homework or any other materials written or drawn by a pupil aside from multiple-choice questions responses
- Lesson plans created by a teacher
- Prompts entered into generative AI tools

We will not allow or cause intellectual property, including students' work, to be used to train generative AI models without appropriate consent or exemption to copyright.

We are aware that secondary infringement could happen if AI products are trained on unlicensed material and outputs and then used in schools or published more widely, such as on the school's website. This may include:

- Publishing a policy that has been created by an AI tool that used input taken from another school's policy without that school's permission
- Using an image on a website that has been created by an AI tool using input taken from the copyright holder without their permission
- Exemptions to copyright are limited – we will seek legal advice if we are unsure as to whether we are acting within the law.

Requirements:

- Teachers must not input student work into an unapproved AI tool (for example ChatGPT or some free plagiarism checkers), as the work produced may be the student's intellectual property and may be retained by the AI system.
- Staff must not share or upload copyrighted material into AI systems unless rights are held.
- AI systems are trained on a range of data, some of which may be copyrighted; we should avoid sharing widely work generated by AI.

14.4 Acceptable usage of artificial intelligence (AI) for students

Our aim is to ensure that students are empowered to use AI responsibly so they are able to take advantage of the opportunities that such tools provide for both work and study, while balancing this with our responsibility to deter plagiarism and exam malpractice in order to maintain academic integrity.

The school aligns its approach to generative AI with the principles set out by the Department for Education in [Generative AI: Product Safety Standards](#). Generative AI will only be used where it demonstrably supports learning, operates safely, and meets data protection and safeguarding requirements.

The school will manage student access to Generative Artificial Intelligence (GenAI) tools in line with safeguarding, data protection, and educational considerations.

Access to a number of GenAI platforms, including but not limited to ChatGPT, Perplexity, Claude, and Microsoft Copilot, will be restricted on the school network and on school-managed devices.

Students in Year 9 and above are permitted access to Google Gemini through their school Google accounts. These accounts will be configured as under-18 educational accounts in order to provide enhanced safeguarding controls, increased oversight, and additional protections designed for educational settings. It operates under the Google Workspace for Education Terms and benefits from the same security protections as core services such as Gmail and Google Docs.

Gemini incorporates enhanced safety and safeguarding controls appropriate for an educational setting. These include age-sensitive guardrails designed to reduce the likelihood of inappropriate or harmful outputs. The platform provides structured onboarding and AI literacy materials to support responsible and informed use by young people, and includes response verification features intended to improve the reliability of factual answers. Administrative oversight, monitoring and management controls are enabled to allow the school to supervise use effectively and respond appropriately to any concerns. In addition, the school's existing filtering and monitoring systems will continue to operate alongside Gemini and will provide oversight of concerning prompts, searches, or typed content in line with existing filtering and monitoring procedures.

Students in Years 7 and 8 will not have access to Google Gemini or other GenAI tools through school systems due to age-related considerations and the relevant terms of service.

The school reserves the right to review, amend, restrict, or expand access to AI tools in response to changes in technology, safeguarding guidance, educational need, or legal and regulatory requirements.

Student use of AI tools should take place within our identified framework outlined in Appendix 1. Teachers can use this to identify the level of acceptable AI use clearly when setting tasks and assignments for students to complete.

Although it is not an expectation for this to be done for every class or home learning assignment, teachers will clearly inform students of the specific regulations on AI use for non-examination assessment as the rules may depend on the qualification.

14.5 Academic Integrity

AI can be misused in 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.

Teachers should:

- Follow JCQ guidance on AI use in examined assessments
- Understand that AI detection tools are usually ineffective and only approved tools should be used for this purpose; other approaches should be considered such as redesigning independent work to make it less easy to complete with AI, or including an element of verbal assessment or personal reflection.

Appendix 1: Your teacher will tell you which level of AI use is appropriate for the task. These levels apply to classwork, home learning, revision, and assessments. For non examination assessment, your teachers will inform you of the specific regulations on AI use – the rules may depend on your qualification.

1. No AI

**You must not use AI at any stage of this task, including planning and preparation.
Any use of AI where it is not permitted will be addressed in line with the relevant school policy/procedure.**

This level is used when your teacher needs to see your own knowledge and skills, such as during in-class assessments, most non-examined assessments, or practice that prepares you for exams. All of your work, at every stage, must be completed independently, without any AI support. Misusing AI is cheating and a form of malpractice.

2. AI Permitted

Where AI is permitted you must check the output carefully, not copy content directly and clearly acknowledge where you have used AI by referencing correctly.



a. AI Planning

You may use AI to help you get started.

This level supports preparation of work, not completion of work.

- Brainstorming ideas
- Creating an outline or plan
- Generating questions to research
- Suggesting sources of information to explore

Your final work must be entirely written or created by you, showing your own thinking and understanding.



b. AI Collaboration

You may use AI to support the creation of parts of your work.

This level supports improvement and development of your work.

- Improving clarity, structure and readability
- Checking for spelling or grammar
- Asking for examples or explanations to deepen your understanding
- Using AI to check whether your work meets the success criteria

Your final work must be clearly your own, showing your decisions, edits, and understanding.



c. AI Exploration

You may use AI to experiment with ideas and solve problems.

This level supports creative thinking and deeper learning, not replacing your own reasoning.

- Exploring alternative solutions or interpretations
- Testing different approaches to a task or problem
- Asking “what if...?” questions to stretch thinking
- Using AI to extend or challenge your ideas

Your final work must show your thought process, including choices you made based on AI’s suggestions.



d. Full AI

You may use AI throughout the task as directed, unless your teacher sets limits.

This level supports full integration of AI while keeping you in control of decisions and output.

- Using AI for planning, drafting, and refining your work
- Using AI to explain, summarise, or suggest improvements
- Using AI to generate media e.g. logos, diagrams, images
- Using AI for research, problem-solving, and evaluation

Your final work must still demonstrate your understanding, accuracy, and ability to direct AI effectively.



Beaumont School

Acceptable use of the school's ICT systems and internet: agreement for students

This agreement explains how I must behave when I use school technology, devices, and the internet, both in school and when my actions outside school affect members of the school community. By using any school technology or accessing school systems, I agree to follow these rules:

1. Using school IT systems safely and responsibly

I will:	I will not:
- Use school ICT systems, Chromebooks, online platforms, and the internet responsibly and for learning purposes only. - Keep usernames/passwords private and secure. - Respect other people's privacy and never try to access files, accounts, or personal information that are not mine. - Log off or shut down computers and devices when I have finished using them. - Follow all instructions from staff about when and how devices should be used in lessons.	- Access or attempt to access inappropriate, harmful, extremist, or illegal material. - Use VPNs, proxies, personal hotspots, or 4G/5G connections to bypass filtering or monitoring. - Install or download software, apps, or browser extensions without permission. - Attempt to alter or disable security settings on any school device. - Cause physical damage to school ICT equipment. - Use anyone else's password or attempt to access another student's account.

2. Online behaviour, communication and reputation

I will:	I will not:
- Make sure all my online communication is responsible, respectful and sensible. - Report anything that makes me or someone else feel uncomfortable, upset, or unsafe to a teacher (in school) or a trusted adult (out of school). - Understand that everything I access, search for, post or receive on school systems can be monitored, logged and, if necessary, shared with parents, carers or the police.	- Use rude, offensive, discriminatory, threatening, or unkind language. - Post or share anything online that could embarrass, upset, or harm someone else. - Take, record, share or livestream photos, videos or audio of students, staff or lessons without permission from a teacher and all people involved. - Do anything online that could bring the school into disrepute, even outside school hours.

3. Personal information and online safety

I will:	I will not:
- Keep my personal information safe and never share my full name, address, phone number or school details without permission from a teacher or parent/carers. - Report any request for personal information from someone I don't know in real life. - Check information carefully and not assume that everything online is true.	- Arrange to meet anyone I only know online without permission from a parent/carers and without adult supervision. - Lie about my age to access age-restricted apps, games or social media sites.

4. Artificial Intelligence (AI) tools

I will:	I will not:
- Follow the AI level my teacher tells me to use for each task (No AI, Planning, Collaboration, Exploration or Full AI) - Comply with all exam-board regulations for NEA. - Complete all work independently when AI is not permitted. - Check AI output carefully and think critically about it. - Acknowledge and reference any AI use correctly when required.	- Use AI when my teacher has said it is not allowed. - Copy or present AI-generated work as my own. - Use AI to generate harmful, inappropriate, misleading or offensive content.

5. Mobile phones and personal devices

I will:	I will not:
- Follow the school's rules on mobile phones and associated devices (tablets, smartwatches, smart glasses). - Use the school's guest WiFi to connect any personal device used for learning e.g. tablet or laptop (Sixth Form students)	- Use, show, or allow my phone or any associated device (smartwatch, tablet, smart glasses) to make noise during the school day (Years 7-11) - Use my phone outside the designated Sixth Form areas if I am a Sixth Form student. - Use my phone in a Sixth Form lesson without the teacher's explicit permission.

6. Use of School-Issued Chromebooks (including 1:1 Device Scheme for Year 7 in September 2026)

I will:	I will not:
- Bring my Chromebook to school each day, fully charged and ready for learning. - Use it for schoolwork and follow teachers' instructions about when and how the Chromebook should be used in lessons. - Keep it safe, secure and stored appropriately when not in use. - Report any damage, faults or issues as soon as possible to the IT department - Log in with my own school account and use the school WiFi on site.	- Use the Chromebook for gaming, social media or non-school activities during the school day. - Use the Chromebook outside of lesson time or a designated activity (e.g. relevant lunch time club) - Install or attempt to install unapproved apps, extensions, software or media. - Tamper with or bypass filtering, monitoring, security or management settings. - Lend the Chromebook to others or allow anyone else to use it. - Reset, wipe or attempt to remove the Chromebook's management controls.

I have read and understood the rules in this Acceptable Use Agreement. I understand that these rules are designed to keep me safe, support my learning and protect others in the school community.

By signing this agreement, I accept that:

- I must follow these rules whenever I use school systems, devices, accounts or networks.
- These rules apply in school, at home and on trips, whenever I am using school technology or representing the school online.
- If I break these rules, the school may take action in line with its behaviour, safeguarding and digital conduct policies, and my parents/carers may be contacted.
- In serious cases, devices may be confiscated, access to systems may be restricted, and external agencies (including the police) may be informed if required by law.

Student Signature		Date	
Student Name		Form	



Beaumont School

Acceptable use of the school's ICT systems and internet: agreement for staff

This Acceptable Use Agreement sets out the expectations for safe, secure and responsible use of the school's ICT systems, devices, online services and internet access. It applies when using school systems on-site or off-site, and when using personal devices for any school-related purpose.

All staff, student teachers and trustees are expected to adhere to this agreement and to the Online Safety and Digital Conduct Policy. Any concerns or clarification should be discussed with Danielle Irving (Assistant Headteacher) or Andy Gray (Assistant Headteacher). Safeguarding concerns must be reported to Danielle Irving (DSL) or a deputy (see Child Protection Policy). Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply, and police involvement will be sought.

By using school ICT systems or accessing the internet on a school network or device, I agree to follow all of the rules below.

1. Using school IT systems safely and responsibly

I will:	I will not:
• Use school ICT systems and online platforms only for professional, educational or school-related purposes. • Use a school-issued device primarily for business use; all other uses are secondary and must not interfere with my work duties or breach any other school policies. Only "insignificant" personal use is permitted, examples of which might include checking personal email or online banking. • Follow all staff instructions and school policies relating to ICT, data protection, online safety and digital conduct. • Log out of accounts and lock devices whenever they are unattended. • Report any concerns about online safety, harmful content or behaviour that may put students or staff at risk. • Ensure that any personal device used for school purposes is password-protected, kept secure, has up-to-date security settings and is used only by me. • Ensure that my online activity, both inside and outside school, does not bring the school, my professional reputation, or that of others into disrepute. • Pre-check all internet sites used in lessons and ensure no unsuitable material (including adverts or pop-ups) is visible. • Follow the requirement to secure advance approval from Danielle Irving or Andy Gray whenever I use controversial or sensitive material as part of teaching. • Follow all cyber security advice and keep up to date with cyber security training as required.	• Access, create, store, share or link to inappropriate, illegal, extremist, violent, discriminatory or pornographic material. • Attempt to access areas of the system, networks or data that I am not authorised to access. • Attempt to bypass filters or monitoring systems, including through VPNs, proxies or personal hotspots. • Free-surf or search the internet in front of students. • Use ICT systems in any way that could damage the school's reputation.

2. Use of email, communication and social media

I will:	I will not:
• Use school-provided email and communication platforms for all school business. • Communicate with students, parents/carers and families professionally, and only through official school systems. • Report phishing attempts, suspicious emails or potential security breaches immediately. • Understand that all email use may be monitored and must be available to my line manager, headteacher or others as required.	• Use personal emails, messaging services or social media to communicate with students or their families. • Use my school email address for personal matters or non-school business. • Post images, information or opinions about students, staff, school activities or members of the school community on personal social media. • Forward confidential information to a personal account or share it without authorisation.

3. Social networking and online reputation

I will:	I will not:
• Keep my personal accounts private and ensure privacy settings remain appropriately secure • Ensure that any 'outward facing' element of social media e.g. profile picture is appropriate.	• "Friend", "follow" or engage in private messaging with students on any social networking platform. • Have private online contact with parents/carers where my school role is the only connection. • Post anything online that undermines the school, its staff, trustees, parents or students. • Share privileged, confidential or sensitive information on personal platforms.

4. Data protection, privacy and information security

I will:	I will not:
• Follow the school's Data Protection Policy at all times, including principles of data minimisation and secure handling. • Store work files only on school-approved systems, including cloud storage and shared drives. • Immediately report lost or stolen devices to IT • Immediately report accidental disclosure of personal data or any suspected data breach to the DPO. • Ensure personal or sensitive data taken off site is encrypted and authorised.	• Access, share, edit or delete personal data unless I am authorised to do so. • Transfer school data to personal cloud accounts or unsecured personal devices. • Leave screens or devices where unauthorised individuals could view them. • Leave school-owned devices unsecured in an accessible or visible location when unattended. • Share login details for any school platform with anyone. • Use external devices e.g. removable storage devices without consent from IT

5. Use of Artificial Intelligence (AI)

I will:	I will not:
• Use AI tools only when permitted and only in ways that comply with the school's Online Safety and Digital Conduct Policy. • Ensure that any output created with AI is checked for accuracy, appropriateness, bias and suitability before being used for any school purpose.	• Input, upload or share personal, sensitive or confidential pupil or staff information with any AI system unless explicitly authorised and compliant with data protection requirements. • Use AI tools to carry out tasks that must reflect my own professional judgement.

6. Mobile phones, personal devices and removable media

I will:	I will not:
---------	-------------

• Use personal devices in school only in accordance with the school's Online Safety and Digital Conduct Policy and staff mobile phone expectations. • Take all appropriate steps to ensure that any device used for school purposes remains secure, password-protected, and used only by me. • Store work data only on school-approved platforms and ensure that any removable media (e.g. USB drives) is encrypted and authorised for use. • Take care not to put myself in a position where a safeguarding allegation can be made as a result of my use of personal devices.	• Use work devices for any personal, non-school activity beyond what is permitted as insignificant personal use. • Share work devices with family or friends, or allow others to access school accounts. • Use personal devices to store, process or share school data unless expressly authorised and compliant with school policy. • Use personal hotspots, VPNs, proxies or other methods to bypass school filtering and monitoring systems.
---	--

7. Digital content, copyright and school property	
I will:	I will not:
• Respect copyright, licensing and intellectual property rights. • Use only legally acquired, authorised digital resources and software. • Take photographs or videos of students only when authorised and only where appropriate consent exists, using school equipment wherever possible. • Transfer any images taken on a personal device to the school network immediately on return to school and delete them from the personal device and cloud storage.	• Use unauthorised software, resources or digital tools. • Upload images or videos of students, staff or parents/carers except on approved school platforms in accordance with photo consent.

8. Additional hardware, software and online tools	
I will:	I will not:
• Seek approval from Rob Leigh (Network Manager) before installing any software or connecting hardware to the school network.	• Subscribe to or encourage students to subscribe to online services for use in school without approval from Danielle Irving or Andy Gray and a proper assessment of risks.

9. Promoting online safety	
I will:	
• Promote positive online safety messages when teaching, setting homework or providing pastoral support. • Report inappropriate or concerning online behaviour (staff, trustees, students, parents or visitors) to the DSL. • Support the school's whole-school safeguarding approach.	

10. Video conferencing and remote teaching	
I will:	
• Only use conferencing tools that have been risk-assessed and approved by the school • Use a school-owned device when running video conferences whenever possible. • Ensure a neutral background to avoid sharing confidential or sensitive information.	

I understand that the school monitors all use of ICT systems, including internet activity, email, and device activity. I understand that misuse of ICT systems, including breaches of this agreement, may result in disciplinary action in line with school policy, and may involve referral to external agencies where appropriate.

Declaration: I have read and understood this Acceptable Use Agreement and agree to follow it and to support online safety throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment.



Beaumont School

Acceptable use of the school's ICT systems and internet: agreement for trustees and members

This Acceptable Use Agreement outlines expectations for safe, secure and responsible use of school ICT systems, information, online services and digital communication by trustees and members. It applies when accessing school systems on-site or off-site, including cloud platforms, email, online meeting tools and any digital documentation related to governance.

By accessing any school information or systems, I agree to the following:

1. Professional conduct and online reputation

I will:	I will not:
- Ensure my online activity does not bring the school, students, staff, trustees, members or myself into disrepute. - Maintain clear professional boundaries and ensure my role as trustee or member is reflected in any online behaviour.	- Post negative, confidential or sensitive information about the school, staff, students or the wider community on personal social media. - Engage in online behaviour that undermines the reputation of the school or board of trustees.

2. Use of email, communication and social media

I will:	I will not:
- Use only official channels or school-authorised communication tools for governance communication. - Keep personal social media accounts private and secure.	- Have private online contact, follow, friend or message students at any time, where my school role as a trustee or member is the only connection. - Use personal emails or messaging apps to store or share governance information.

3. Data protection, confidentiality and information security

I will:	I will not:
- Follow the school's Data Protection Policy, GDPR requirements and confidentiality expectations. - Access governance papers only through approved platforms e.g. secure school email. - Store digital documents securely and ensure they are not accessible to anyone else. - Report any lost devices, accidental disclosures, or suspected data breaches immediately to the Clerk and Data Protection Officer. - Ensure any device used to access governance material is secure, password-protected and updated.	- Forward confidential governance documents to personal cloud storage or non-secure accounts. - Share, print or store sensitive information where unauthorised individuals may access it. - Access, share or delete personal or sensitive data unless required and authorised as part of my duties as a trustee.

4. Cybersecurity and safe access

I will:	I will not:
- Follow cyber-security expectations set out by the school and local authority. - Use strong, unique passwords and keep them confidential. - Report phishing attempts, suspicious emails or potential cyber threats immediately. - Use only secure internet connections (not public Wi-Fi) when accessing confidential documents. - Follow all cyber security advice and keep up to date with cyber security training as required.	- Attempt to bypass any security measures, filters or controls. - Share login details for any school platform with anyone.

5. Use of Artificial Intelligence (AI)

I will:	I will not:
- Use AI tools responsibly and only to support governance tasks where appropriate - Check all AI-generated information for accuracy and bias before using it in governance work. - Ensure no personal data, confidential documents or sensitive information is input into any AI system unless this is permitted and compliant with data protection requirements.	- Use AI to analyse or process personal data about students or staff. - Allow AI tools to form judgements about school performance, individual students or staff.

6. Use of devices

I will:	I will not:
- Ensure any personal device used for governance work is secure, password-protected and used only by me. - Enable automatic updates and antivirus/security protections.	- Allow others, including family members, to access devices or accounts used for governance. - Download unapproved software or connect unauthorised hardware to school ICT systems.

I understand that:

- The school may monitor use of its ICT systems and online platforms.
- Any breach of this agreement may result in action by the Board of Trustees in line with governance procedures.
- Serious breaches may be referred to external agencies where appropriate.

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school. I understand this forms part of my responsibilities as a trustee or member.