Malmesbury School E-Safety Policy

Date of Review	Approved by	Date of Approval	Next Review Date	Website
February 2026	Governors	5 February 2026	November 2027	Y

Aims

At Malmesbury School, we embrace the use of ICT and recognise that we play a key role in ensuring that children and adults are well informed and equipped to use this safely. This policy applies to all members of the immediate and extended school community who have access to and are users of school ICT systems.

We aim 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
- establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

1. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, **Keeping Children Safe in Education**, **Cyber Security Standards for Schools and Colleges**, **The Department for Education's filtering and monitoring standards**, **Online Safety Training For Schools | The National College** and its advice for schools. The policy also considers the National Curriculum computing programmes of study.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **contact:** being subjected to harmful online interaction with other users; for example: 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; for example, 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. Roles and responsibilities

2.1 Local Governing Body

The Cyber Governor, Governors and the Designated Safeguarding Lead (DSL) are responsible for monitoring this policy by discussing audits, incident logs and online access and provision.

All governors will:

- ensure they have read and understood this policy
- recognise the links to other policies, to include –

  Athelstan Trust Child Protection and Safeguarding Policy
  IT Acceptable Use Policy (Trust document – Employment Manual)
  Athelstan Trust Code of Conduct (Trust document – Employment Manual)

2.2 The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently. Day-to-day responsibility for online safety will be delegated to the DSL. The Headteacher/Senior Leaders are responsible for ensuring that the DSL and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

2.3 The Designated Safeguarding Lead

The role of the DSL and Deputy Designated Safeguarding Leads (DDSLs) 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, network manager and other staff, as necessary, to address any online safety issues or incidents
- 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
- Liaising with other agencies and/or external services if necessary
- Test the monitoring and filtering systems to ensure its effectiveness

This list is not intended to be exhaustive.

2.4 The Network Manager / Technical staff

The network manager/technical staff are responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis. The system must keep pupils 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 regular 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 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
- Ensure use of Generative AI in school is in line with the DofE's Generative AI: product safety expectations so that artificial intelligence is used safely, and that filtering and monitoring requirements are sufficient

This list is not intended to be exhaustive.

2.5 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 as outlined in the Athelstan Trust Employment Manual – IT Acceptable Use Policy (appendix 1), Athelstan Trust Employment Manual – Social Media Policy (appendix 2) and ensuring that pupils follow the terms in the Student ICT Acceptable Use Policy (appendix 3)
- Working with the DSL and DDSLs to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Trust's behaviour policy
- Engaging with E-Safety training where appropriate

This list is not intended to be exhaustive.

2.6 Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local E-Safety campaigns/literature.

Parents are expected to:

- Notify a member of staff if they have concerns about E-Safety
- Ensure their child has read, understood and agreed to the terms on acceptable use (appendix 3)

Parents 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**

2.7 Visitors and members of the community

Visitors and members of the community who use the academy'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.

3. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum: From September 2020 all schools will have to teach: **Relationships and sex education and health education** in secondary schools

E-Safety education will be provided in the following ways:

- A planned E-Safety programme should be provided as part of Computing/PHSE/other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key E-Safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Students should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Students should be helped to understand the need for the Student ICT Acceptable Use Policy, encouraged to adopt safe and responsible use of ICT, the internet and mobile devices, both within and outside school.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students should be taught to be cautious of content online that could be disinformation, misinformation or conspiracy theories and the importance of fact checking information

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

- Their rights, responsibilities, and opportunities online. This will include an understanding that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content

- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How to identify disinformation, misinformation and conspiracy theories

4. Educating parents about online safety

Malmesbury School will provide information and raise parents' awareness of internet safety in letters or other communications home, and in information via the school website. Online safety will also be covered during parents' information evenings, such as The New Year 7 Information Evening and specifically arranged events designed to address elements of E-Safety. These events will involve outside speakers where it is beneficial to do so.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL. Concerns or queries about this policy can be raised with any member of staff.

5. Cyber-bullying

5.1 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. (Also see the school behaviour policy.)

5.2 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.

Malmesbury School will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Tutors will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

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

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. Specific consideration will also be given to the safeguarding policy – peer on peer abuse. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable efforts 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.

5.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, 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
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on **screening, searching and confiscation.**

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. Acceptable use of the internet in school

All members of the community who use the 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.

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 agreements.

7. Pupils using mobile devices in school

Pupils may bring mobile devices to school but are not permitted to use them during the school day (8.55am-3.25pm). Mobile devices should be off and in bags and can only be used if directed by a member of staff.

Phones should not be used for clubs before or after school, or any other activities organised by the school (unless agreed by teacher for a planned activity, such as a school trip/exchange).

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement.

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 the device.

8. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way that would violate the school's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of the work device when using it outside school. Any USB devices containing data relating to the school must be encrypted. Any loss of data must be immediately reported to the Data Protection Officer as per GDPR.

If staff have any concerns over the security of their device, they must seek advice from the network manager. Work devices must be used solely for work activities and staff must agree and adhere to the terms as outlined in the Athelstan Trust Employment Manual – IT Acceptable Use Policy (appendix 1) and the Athelstan Trust Employment Manual – Social Media Policy (appendix 2)

9. How the school will respond to issues of misuse

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

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct and staff disciplinary procedure. 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.

10. 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 and extremism through access to misinformation, disinformation (including fake news) and conspiracy theories.

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).

The DSL and DDSLs 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.

11. Monitoring arrangements

Filtering and monitoring are both important ways of safeguarding pupils and staff from potentially harmful and inappropriate online material.

The school's internet is accessed through the Southwest Grid for Learning and it is constantly being reviewed by local authorities, government, and other external providers.

Live updates are constantly being made to the service, to help protect users.

Impero software monitors all school computer and laptop activity. Details of browsing behaviour and attempted access to inappropriate sites are automatically sent to the network office as a screen shot, along with the identity of the individual who logged onto the device. This ensures that inappropriate use can discussed with individual users. This software is constantly updated live.

In the event of a service disruption to any filtering, the computer or laptop is blocked from being online and presents as “not connected to the internet”.

We believe that the constant review and live updates offered by the Southwest Grid for Learning and Impero, ensures that the level of protection evolves over time, in line with new risks and without the delay that an internal review process would generate.

Any safeguarding concerns will be reported to the DSL or DDSL in line with safeguarding procedures and any inappropriate material which makes its way through the Southwest Grid for Learning will be shared with the organisation and added to their blocked site database.

12. Links with other policies and procedures

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Data Protection Policy and privacy notices
- Complaints procedure
- IT acceptable use policy
- Code of Conduct
- Disciplinary procedure
- Disciplinary rules

Appendix 1

IT acceptable use policy

1 **Introduction: This policy sets out the requirements with which you must comply when using the Trust's IT** and when otherwise using IT in connection with your job including:

1.1 The Trust's email and internet services

1.2 Telephones and faxes

1.3 the use of mobile technology on Trust premises or otherwise in the course of your employment (including 3G / 4G, Bluetooth and other wireless technologies) whether using an Academy, Trust or a personal device; and

1.4 any hardware (such as laptops, printers or mobile phones) or software provided by, or made available by, the Trust.

1.5 This policy also applies to your use of IT off Trust premises if the use involves Personal Information of any member of the Trust community or where the culture or reputation of the Trust or any of its academies are put at risk.

2 **Failure to comply:** Failure to comply will constitute a disciplinary offence and will be dealt with under the Trust's Disciplinary Procedure.

3 **Property:** You should treat any property belonging to the Trust with respect and reasonable care and report any faults or breakages immediately to the Finance Office. You should not use the Trust's computers or other IT resources unless you are competent to do so and should ask for training if you need it.

4 **Viruses and other malicious code:** You should be aware of the potential damage that can be caused by computer viruses and other malicious code. You must not introduce use, introduce or operate any hardware, programmes or data (including computer games) or open suspicious emails which have not first been checked by the Trust for viruses.

5 **Passwords:** Passwords should be long, for example you could use a song lyric or a memorable phrase plus a number. Do not choose a password which is so complex that it's difficult to remember without writing it down. Your password should not be disclosed to anyone else. In addition:

5.1 Your password should be difficult to guess, for example you could base your password on something memorable that no one else would know. You should not use information which other people might know, or be able to find out, such as your address or your birthday.

5.2 You must not use a password which is used for another account. For example, you must not use your password for your private email address or online services for any school account.

5.3 Passwords (and any other security credential you are issued with such as a key fob or USB drive) must be kept secure and confidential and must not be shared with, or given to, anyone else. Passwords should not be written down.

6 **Leaving workstations:** If you leave your workstation for any period of time you should take appropriate action and, in particular, you should log off and / or set your screen saver with an appropriate password.

7 **Concerns**: You have a duty to report any concerns about the use of IT at the Trust to the Headteacher. For example, if you have a concern about IT security or pupils accessing inappropriate material.

8 **Other policies**: This policy should be read alongside the following:

8.1 Code of Conduct

8.2 data protection policy for Staff

8.3 information security policy; and

8.4 acceptable use policy for pupils

Internet

9 **Downloading:** Downloading of any programme or file which is not specifically related to your job is strictly prohibited.

10 **Personal use:** The Trust permits the incidental use of the internet so long as it is kept to a minimum and takes place substantially out of normal working hours. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. If the Trust discovers that excessive periods of time have been spent on the internet provided by the Trust or it has been used for inappropriate purposes (as described in section 14 below) either in or outside working hours, disciplinary action may be taken and internet access may be withdrawn without notice at the discretion of the Headteacher.

11 **Unsuitable material:** Viewing, retrieving or downloading of pornographic, terrorist or extremist material, or any other material which the Trust believes is unsuitable, at any time, is strictly prohibited and constitutes gross misconduct. Internet access may be withdrawn without notice at the discretion of the Headteacher whilst allegations of unsuitable use are investigated by the Trust.

12 **Location services**: The use of location services represents a risk to the personal safety of those within the Trust community, the Trust's security and its reputation. The use of any website or application, whether on a Trust or personal device, with the capability of publicly identifying the user's location while on Trust premises or otherwise in the course of employment is strictly prohibited at all times.

13 **Contracts:** You are not permitted to enter into any contract or subscription on the internet (including through an App) on behalf the Trust or any of its Academies, without specific permission from the Headteacher. This applies both to "free" and paid for contracts, subscriptions and Apps.

14 **Retention periods**: The Trust keeps a record of staff browsing histories for a period of 90 days.

Email

15 **Personal use:** The Trust permits the incidental use of its email systems to send personal emails as long as such use is kept to a minimum and takes place substantially out of normal working hours. Personal emails should be labelled 'personal' in the subject header. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. The Trust may monitor your use of the email system, please see paragraphs 26 to 30 below, and staff should advise those they communicate with that such emails may be monitored. If the Trust discovers that you have breached these requirements, disciplinary action may be taken.

16 **Status:** Email should be treated in the same way as any other form of written communication. Anything that is written in an email is treated in the same way as any form of writing. You should not include anything in an email which is not appropriate to be published generally.

17 **Inappropriate use:** Any email message which is abusive, discriminatory on grounds of sex, marital or civil partnership status, age, race, disability, sexual orientation or religious belief (or otherwise contrary to our equal opportunities policy), or defamatory is not permitted. Use of the email system in this way constitutes gross misconduct. The Trust will take no responsibility for any offence caused by you as a result of downloading, viewing or forwarding inappropriate emails.

18 **Legal proceedings:** You should be aware that emails are disclosable as evidence in court proceedings and even if they are deleted, a copy may exist on a back-up system or other storage area.

19 **Jokes:** Trivial messages and jokes should not be sent or forwarded to the email system. They could cause the Trust's IT system to suffer delays and / or damage or could cause offence.

20 **Contracts:** Contractual commitments via an email correspondence are not allowed without prior authorisation of the Headteacher.

21 **Disclaimer:** All correspondence by email should contain the Trust's disclaimer.

22 **Data protection disclosures:** Subject to a number of limited exceptions, potentially all information about an individual may be disclosed should that individual make a subject access request under data protection legislation. There is no exemption for embarrassing information (for example, an exchange of emails containing gossip about the individual will usually be disclosable). **Staff must be aware that anything they put in an email is potentially disclosable**.

Monitoring

23 The Trust regularly monitors and accesses its IT system for purposes connected with the operation of the Trust. The Trust IT system includes any hardware, software, email account, computer, device or telephone provided by the Trust or used for Trust business. Staff should be aware that the Trust may monitor the contents of a communication (such as the contents of an email).

24 The purposes of such monitoring and accessing include:

24.1 to help the Trust with its day-to-day operations. For example, if a member of staff is on holiday or is off sick, their email account may be monitored in case any urgent emails are received; and

24.2 to check staff compliance with the Trust's policies and procedures and to help the Trust fulfil its legal obligations. For example, to investigate allegations that a member of staff has been using their email account to send abusive or inappropriate messages.

25 Monitoring may be carried out on a random basis, and it may be carried out in response to a specific incident or concern.

26 The Trust also uses software which automatically monitors the Trust IT system (for example, it would raise an alert if a member of Staff visited a blocked website or sent an email containing an inappropriate word or phrase).

27 The monitoring is carried out by the IT Manager. If anything of concern is revealed as a result of such monitoring, then this information may be shared with the Headteacher and CEO and this may result in disciplinary action. In exceptional circumstances concerns will need to be referred to external agencies such as the Police.

Appendix 2

Social Media

1 **Introduction:** The Trust recognises that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media, such as Facebook, Bebo, LinkedIn, Twitter, Instagram, Snapchat and all other internet postings including blogs and wikis and other interactive websites. It is also a valuable educational tool.

2 **Purpose:** This policy applies to the use of social media for Trust and your own personal purposes, whether during normal working hours or in your personal time. Its purpose is to help staff avoid the potential pitfalls of sharing information on such social media sites and should be read in conjunction with the acceptable use policy for pupils.

3 **IT facilities:** The policy applies regardless of whether the social media is accessed using the Trust's IT facilities and equipment or your personal equipment.

4 **Personal use**: The Trust permits the incidental use of the internet and social media so long as it is kept to a minimum and takes place substantially out of normal working hours. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. If the Trust discovers that excessive periods of time have been spent on the internet provided by the Trust either in or outside working hours, disciplinary action may be taken and internet access may be withdrawn without notice at the discretion of the Headteacher.

5 **Guiding principles**: Staff are required to behave responsibly at all times and adhere to the following principles:

6 **You should not be "Friends" with "Followers" or connect with pupils on any social media network.** It would be considered inappropriate to add pupils as Friends on a personal account. Depending on the circumstances, it may also be inappropriate to connect with parents, guardians or carers as Friends.

6.1 You must be mindful of how you present yourself and the Trust and its Academies on such media. Staff are entitled to a social life like anyone else. However, the extra-curricular life of an employee at the Trust has professional consequences and this must be considered at all times when sharing personal information.

6.2 You must not publish anything which could identify pupils, parents or guardians on any personal social media account, personal webpage or similar platform without the prior consent of the Headteacher in writing. This includes photos, videos, or other materials such as pupil work.

6.3 You should always represent your own views and must not allude to other people's personal views in your internet posts.

6.4 When writing an internet post, you should consider whether the contents would be more appropriate in a private message. While you may have strict privacy controls in place, information could still be shared by others. It is always sensible to consider that any information posted may not remain private.

6.5 You should protect your privacy and that of others by omitting personal information from internet posts such as names, email addresses, home or work addresses, phone numbers or other personal information.

6.6 You should familiarise yourself with the privacy settings of any social media you use and ensure that public access is restricted. If you are not clear about how to restrict access, you should regard all your information as publicly available and behave accordingly.

6.7 You must not post anything that may offend, insult or humiliate others, particularly on the basis of their sex, age, race, colour, national origin, religion, or belief, sexual orientation, disability, marital status, pregnancy or maternity.

6.8 You must not post anything that could be interpreted as threatening, intimidating or abusive. Offensive posts or messages may be construed as cyber-bullying.

6.9 You must not post disparaging or derogatory remarks about the Trust, its Academies or its Governors, officers, staff, volunteers, pupils or parents, guardians or carers.

6.10 You must not post anything that could be interpreted as glorifying or supporting terrorism, extremism or organisations promoting terrorist or extremist views, or encouraging others to do so.

6.11 You must not use social media in a way which could constitute a breach of any policies contained in this Employment Manual.

7 **Removing postings:** You may be required to remove internet postings which are deemed to constitute a breach of this policy. If you fail to remove postings, this could result in disciplinary action.

8 **Breach:** A breach of this policy may be treated as misconduct and could result in disciplinary action including in serious cases, dismissal.

9 **Monitoring:** The Trust regularly monitors the use of the internet, social media and email systems to check that the use is in accordance with this policy. Please see the IT acceptable use policy for further information on monitoring. If it is discovered that any of the systems are being abused and / or that the terms of this policy are being infringed, disciplinary action may be taken which could result in your dismissal.

Appendix 3

Malmesbury School Student ICT Acceptable Use Policy

These regulations apply to the use of all Internet and electronic mail facilities, multi-user computers, laptops, workstations and other electronic devices and any networks connecting them provided by Malmesbury School. The school's aim is to ensure students use the school network effectively for its intended purpose, without infringing legal requirements or creating any unnecessary risk.

The facilities must be used only in connection with the student's learning at school, or other educational purposes permitted by the Headteacher. Private use of the Internet is a privilege at school not a right. Students are required to behave in a responsible and appropriate manner at all times. Students must remember that their 'MyWorkspace' is for their sole use and must not gain access to or violate the privacy of other people's files, corrupt or destroy other people's data or disrupt the work of other people. These actions are in breach of the Computer Misuse Act 1990. Under no circumstances may the facilities be used for commercial gain.

This policy applies to the use of all IT equipment and networks provided by, and connected to, Malmesbury School.

As a student I will agree to:

- Use the network as provided by Malmesbury School and not alter any settings or bypass
  any safety mechanisms.
- Use IT facilities for learning and other educational purposes.
- Always behave in a responsible and appropriate manner.
- Be on task during lessons.
- Use 'MyWorkspace' for my sole use and not to gain access to other student's spaces for any purpose whatsoever.
- List and quote clearly all Internet material sources in my work.
- Use IT for appropriate means and not for commercial gain.
- Report any damage found to computers or the network to the Network Supervisors without demonstrating to others any discovered methods of causing such damage.
- Use the Internet for educational purposes and understand that private use of the Internet in school is forbidden.
- Keep my password private and therefore secure.

As a student I will agree NOT to:

Create, transmit or cause to be created or transmitted material which is:

- designed or likely to cause annoyance, inconvenience, needless anxiety or offence
- obscene, offensive, indecent or defamatory.
- Infringement of the copyright of another person.
- Use Malmesbury School network for Internet chat rooms or social networking. sites.
- Play computer games without the express permission of a teacher.

- Allow someone to log-on using my username and password.
- Attempt to install software or copy programs on the network.
- Copy sites from the Internet into my own use areas and storage devices.
- Download sites from the Internet outside of school and bring to school to upload.
- Gain deliberate, unauthorized access to facilities or services accessible vial local or national networks.
- Damage computers, computer systems or networks.
- Give out any personal information relating to any member of staff or student at Malmesbury School.
- Publish names or photographs of any member of staff or student on the Internet unless there are exceptional circumstances for which permission is given by a senior member of staff.
- Remove work from or alter work saved in shared areas that I do not own.
- Use AI products in lessons or for work that are not approved for use in school.

Please Note

Cyber bullying will be dealt with in accordance with the school's bullying policy.

Breaches of this policy will be regarded very seriously and comply with the school's behavioural policy and its sanctions, which may include replacement costs. Students may find their access withdrawn and persistent misuse of the network could lead to exclusion from school

Network Supervisors will have the right to gain access to all files and to delete any inappropriate material.

Parent / Student Computer Acceptable Use Policy Agreement

Name of student _____Tutor Group _____

I/we have read, discussed and accept the regulations governing the use of computer facilities.

I/we give our son/daughter permission to have access to the Network and other computing facilities and understand that failure to abide by the policy may result in the withdrawal of these facilities.

Signed _____
(Parent/Guardian)

Signed _____ (Student)

Date _____