THOMAS MILLS HIGH SCHOOL

POLICY DOCUMENT – 53

USE OF TECHNOLOGY POLICY Incorporating GUIDANCE FOR STAFF ON THE USE OF EMAIL/ONLINE CONDUCT

Date approved by Board of Trustees	17/10/2023
Next review due:	Academic Year 2026 - 2027
Policy review cycle:	Every 3 years
Policy Owner:	Deputy Headteacher / IT Manager / Business Manager

Vision Statement

We, the staff and governors, aspire
to ensure that all our students,
irrespective of ability
and regardless of anyone's doubts,
achieve their potential in full;
and we aspire in this way to make Thomas Mills High School
the best in the country.

Contents:

Statement of intent

At Thomas Mills High School, we recognise that the use of artificial intelligence (AI) can help to positively affect teacher workload, develop pupils' intellectual capabilities and prepare them for how emerging technologies will change workplaces. While there are many benefits to the use of AI tools, the content they produce may not always be accurate, safe or appropriate, and could lead to malpractice.

Through the measures outlined in this policy, the school aims to ensure that AI is used effectively, safely and appropriately to deliver excellent education that prepares our pupils to contribute to society and the future workplace.

For the purposes of this policy, the following terms are defined as:

- **AI** – The theory and development of computer systems able to perform tasks normally requiring human intelligence, e.g. visual perception, speech recognition, decision-making.
- **Generative AI** – A category of AI algorithms that generate new outputs based on the data they have been trained on.
- **Misuse of AI** – Any use of AI which means that pupils have not independently demonstrated their own attainment.

1. Artificial Intelligence (AI)

1.1 Using AI tools

The school will ensure that AI tools are used appropriately to achieve the following aims:

- To reduce workload
- To free up teachers' time
- To produce high-quality and compliant administrative plans, policies and documents
- To support the teaching of a knowledge-rich computing curriculum
- To teach pupils:
    - How to use emerging technologies safely and appropriately.
    - About the limitations, reliability and potential bias of AI tools.
    - How information on the internet is organised and ranked.
    - How online safety practices can protect against harmful and misleading content.
    - To identify and use appropriate resources to support their education, including age-appropriate resources and preventing over-reliance on a limited number of tools or resources.

Where AI tools are used to produce administrative plans, policies and documents, all staff members will understand that the quality and content of the final document remains the professional responsibility of the staff member who produced it. Staff members using AI tools to create documents will not assume that AI output will be comparable with a human-designed document that has been developed in the specific context of the school.

Pupils will be made aware of the importance of referencing AI tools correctly when using AI tools to produce work, especially if the work is for an assessment, in order to allow teachers and assessors to review how AI has been used and whether it was appropriate. Pupils' references to AI sources will show the name of the AI source and the date that the content was generated.

Pupils will retain a copy of the questions and AI generated content for reference and authentication purposes in a non-editable format, e.g. a screenshot. Pupils will also provide a brief explanation of how AI tools have been used.

1.2 Misusing AI tools

Preventing misuse

The school acknowledges that misuse of AI tools can happen both accidentally and intentionally, and that education and awareness is key to preventing misuse. The school will consider taking the following actions to prevent the misuse of AI tools:

- Restricting access to online AI tools on school devices and networks, especially on devices used for exams and assessments
- Setting reasonable deadlines for submission of work and providing pupils with regular reminders
- Allocating time for sufficient portions of pupils' work to be completed in class under direct supervision, where appropriate
- Examining intermediate stages in the production of pupils' work to ensure that work is being completed in a planned and timely manner, and that work submitted represents a natural continuation of earlier stages
- Introducing classroom activities that use the level of knowledge and understanding achieved during lessons to ensure the teacher is confident that pupils understand the material
- Engaging pupils in verbal discussions about their work to ascertain that they understand it and that it reflects their own independent work
- Refusing to accept work that is suspected to have been generated through misuse of AI tools without further investigation
- Issuing tasks which are, wherever possible, topical, current and specific, and require the creation of content which is less likely to be accessible to AI models
- Investing in educating and training staff, pupils and parents on the use of AI tools and raising awareness of the risks and issues that come with its use

Identifying misuse

Staff members will continue to use the skills and observation techniques already in use to assure themselves that pupils' work is authentically their own when attempting to identify a misuse of AI tools.

When reviewing pupils' work to ensure its authenticity, staff members will compare it against other work created by the pupil. Where the work is made up by writing, the staff members will make note of:

- Spelling and punctuation.
- Grammatical usage.
- Writing style and tone.
- Vocabulary.
- Complexity and coherency.
- General understanding and working level.
- The mode of production, i.e. whether the work was handwritten or word-processed.

Staff members will be aware of and look out for potential indicators of AI use, which include:

- A default use of American spelling, currency, terms and other localisations.
- A default use of language or vocabulary which might not appropriate to the working or qualification level.
- A lack of direct quotations and/or use of references where these are required or expected.
- Inclusion of references which cannot be found or verified.
- A lack of reference to events occurring after a certain date, reflecting when an AI tool's data source was compiled.
- Instances of incorrect or inconsistent use of first-person and third-person perspective where AI generated text has been left unaltered.
- A variation in the style of language evidenced in a piece of work, if a pupil has taken specific portions of text from an AI tool and then amended it.
- A lack of graphs, data tables or visual aids where these would normally be expected.
- A lack of specific, local or topical knowledge.
- Content being more generic in nature.
- The inadvertent inclusion of warnings or provisos produced by AI tools to highlight the limits of its ability or the hypothetical nature of its output.
- The submission of pupil work in a typed format, where this is not usual, expected or required.
- The unusual use of several concluding statements throughout the text, or several repetitions of an overarching essay structure within a single lengthy essay.
- The inclusion of confidently incorrect statements within otherwise cohesive content.

Staff members will remain aware that AI tools can be instructed to employ different languages and levels of proficiency when generating content, and some are able to produce quotations and references.

Where necessary, the school will make use of the following programmes and services that are able to analyse content and determine the likelihood that it was produced by AI:

- OpenAI Classifer
- GPTZero
- The Giant Language Model Test Room (GLTR)

1.3 Exams and assessments

The school will continue to take reasonable steps where applicable to prevent malpractice involving the use of generative AI tools regarding exams and assessments. The school will follow the Examination: Remarking & Resitting Policy at all times and ensure that these policies address the appropriate and inappropriate use of AI tools.

Pupils will be made aware of the appropriate and inappropriate uses of AI tools, and the consequences of its misuse. Pupils will be made aware that it is not acceptable to submit work that has been produced with an AI tool, and of the school's approach to plagiarism and malpractice. Pupils will also be made aware of the risks of using AI tools to complete exams and assessments, which include:

- Submitting work that is incorrect or biased.
- Submitting work that provides dangerous and/or harmful answers.
- Submitting work that contains fake references.

The school will ensure that pupils are issued with, and fully understand, the JCQ Information for Candidates.

Teachers, assessors and other relevant staff members will discuss the use of AI tools and agree a joint approach to managing pupils' use of AI tools in the school.

Pupils will only be permitted to use AI tools to assist with assessments where the conditions of the assessment permit the use of the internet, and where the pupil is able to demonstrate that the final submission is the product of their own independent work and thinking.

Pupils will be required to sign a declaration to confirm that they understand what AI misuse is, and that it is unacceptable. Pupils will be made aware of the consequences of submitting a false declaration, and any AI misuse that is detected after a declaration has been signed will be reported to the relevant awarding organisation. The misuse of AI constitutes malpractice, as defined in the JCQ 'Suspected Malpractice: Policies and Procedures'. Pupils will be made aware that possible sanctions for committing malpractice through the misuse of AI tools include disqualification and debarment from taking qualifications for a number of years, and that their marks may also be affected. Misuse of AI tools includes, but is not limited to, the following:

- Copying or paraphrasing sections, or whole responses, of AI generated content
- Using AI to complete parts of the assessment so that the work does not reflect the pupil's own work, analysis, evaluation or calculations
- Failing to acknowledge the use of AI tools when they have been used as a source of information
- Incomplete or poor acknowledgement of AI tools
- Submitting work with intentionally incomplete or misleading references and/or bibliographies

The school will not, under any circumstances, accept work which is not the pupils' own.

1.4 Safeguarding

The school acknowledges that generative AI tools can be used to produce content that is dangerous, harmful, and inappropriate. The school will follow the procedures set out in the Safeguarding & Child Protection and the Social Media & Online Safety Policy to ensure that pupils are not able to access or be exposed to harmful content.

Pupils will be taught about the risks of using AI tools and how to use them safely. Pupils will be made aware of how to report any concerns or incidents involving generative AI, and who to talk to about any issues regarding the use of AI tools.

The school will engage with parents via to inform them of the safeguarding risks that come with using AI tools, and the internet in general, and how the school is protecting pupils online. The school will ensure that parents are aware of who to speak to about any concerns or issues regarding the use of AI or Internet Safety.

The school will ensure that the appropriate filtering and monitoring systems are in place to protect pupils online, following the DfE's filtering and monitoring standards.

2. Online Safety

2.1 Educating pupils about online safety

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

In **Key Stage 3**, pupils will be taught to:

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

Pupils in **Key Stage 4** will be taught:

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

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

- Their rights, responsibilities and opportunities online, including 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 people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

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

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

2.2 Educating parents about online safety

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

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.

2.3 Cyber-bullying

2.3.1 Definition

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

2.3.2 Preventing and addressing cyber-bullying

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

The 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.

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

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

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

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

2.3.3 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*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

2.4 Acceptable use of the internet in school

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

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

We will monitor the websites visited by pupils, staff, volunteers, Trustees and visitors (where relevant) to ensure they comply with the above.

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

2.5 Pupils using mobile devices in school

MOBILE PHONE PROTOCOL YEARS 7 – 11

Unlike many schools, Thomas Mills High School permits pupils to bring mobile phones into school. It is certainly a privilege and one which must not be abused.

Pupils are expected to abide by the following:

Mobile phones should not be seen in pupils' possession throughout the school day – no pupil phones should be seen in school.

The only exceptions are:

• When placing mobile phones in the valuables box in PE lessons

• At the end of a lesson, when permitted by a teacher, for photographing what has been displayed on a whiteboard in class

• When handing in phones before entering an exam room.

Hence, phones should not be heard, or used to receive or send text messages at all, nor to access the internet.

The school accepts no responsibility for any personal belongings (including phones) brought into school.

There is a public telephone available to pupils, at the Reception desk, requiring a minimum of 20p for calls.

Sixth Form students are not bound by the same restrictions regarding phone use as Main School pupils. However, phones should not be on display in corridors nor used for photographs of anyone, staff or student, without the express permission of that person, nor should Sixth Form students make their phones available to others.

2.6 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
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Making school devices available on request by the IT Dept or Senior Management within a prompt timeframe.
- Not installing any applications or software that have not been assessed and approved by the IT Manager.
- No confidential data to be stored on any personal devices.
- No confidential data to be stored on CDs, DVDs or USB media unless explicitly required. (e.g. USB media required to be sent to exam boards for assessments.)

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Work devices must be used solely for work activities.

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

2.7 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 disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

2.8 Training

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

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

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

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

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

The DSL 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.

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.

2.9 Monitoring arrangements

The DSL logs safeguarding issues related to online safety.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the Trustee board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

2.10 Links with other policies

This online safety policy is linked to our:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct

- Data protection policy and privacy notices
- Complaints procedure

3. Social Media

To ensure clarity of use and guidance for staff, pupils and all users regarding the use of social media and networking applications.

This guidance is designed to protect individual members of staff, pupils and all users.

This policy applies to the use of social media for both business and personal purposes, whether during School / working hours or otherwise. This policy applies regardless of whether the social media is accessed using school IT facilities and equipment or equipment belonging to members of staff, pupils or any other IT/internet enabled equipment.

Anyone setting up a social media account that is directly connected to Thomas Mills High School (TMHS) (using the name of TMHS, a TMHS School logo, or clearly attached to TMHS in some way) must follow all the guidelines in this policy.

All staff and pupils must read, understand and this policy. New staff will be asked to confirm that they have read and understood.

3.1 Rationale

The widespread availability and use of social media applications bring opportunities to understand, engage, and communicate in new, relevant and exciting ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with duties to the School, the community, out legal responsibilities and our reputation.

The School use of social networking applications has implications for our duty to safeguardchildren, young people and vulnerable adults.

The policy requirements in this document aim to provide this balance to support innovation whilst providing a framework of good practice. They apply to all members of staff and pupils at both Main School and Sixth Form.

The purpose of the policy is to:

- Safeguard all pupils and promote wellbeing;
- Ensure users are not exposed to risk as a result of their actions;
- Use social media in a respectful, positive and productive way which respects all parties involved;
- Ensure that the reputation of TMHS (the School), its staff and Trustees is protected and that stakeholders understand their ambassadorial role with regard to theSchool;
- Protect the School from legal risks;
- Ensure that any users are able clearly to distinguish where information provided via social media is legitimately representative of the School.

3.2 Definitions and Scope

The School defines social media as 'any websites and applications that enable users to create and share content or to participate in social networking'. Social networking sites andtools include, but are not limited to, Facebook, Twitter, Snapchat, TikTok, LinkedIn, MySpace, Flickr, YouTube and Instagram. It also includes forums and discussion boards such as Yahoo! Groups or Google Groups, online encyclopaedias such as Wikipedia, and any other web sites which allow individual users or organisations to use simple publishing tools.

Many of the principles of this policy also apply to other types of online presence such as virtual worlds.

All members of the School should bear in mind that information they share through social networking applications, even if they are on private spaces, may be subject to copyright, safeguarding and data protection legislation. They must also operate in line with other relevant school policies.

3.3 School-sanctioned use of social media and/or social media accounts using the name of Thomas Mills High School, a TMHS School logo, or clearly attached to TMHS School in some way

There are many legitimate uses of social media within the curriculum, and to support student learning and to share news with the wider school community. For example, the School and sub-departments of the School may have official Twitter, Instagram and Facebook accounts and several A-level courses require the use of blogs for assessment. There are also many possibilities for using social media to enhance and develop pupils' learning and to keep the School Community and our supporters in touch with the School.

When using school social media accounts and/or social media accounts using the name of TMHS, a School logo, or clearly attached to the School in some way, the following practices must be observed:

3.3.1 A distinct and dedicated social media site or account must only set up with the permission of the AH & Online safety Officer or Business Manager. This should be entirely separate from any personal socialmedia accounts held and should be linked to an official school email account. Social media accounts must have a link to this Policy, have official TMHS branding and state that it is an 'Official TMHS School Approved Site'. If a social media account is identified (that uses the name of TMHS, a TMHS logo, or clearlyattached to TMHS in some way) that is not an official TMHS approved site, this should be reported to the Business Manager.

3.3.2 The social media account must be approved by the appropriate Head or SMT and updates to passwords must be shared with the Media Committee.

3.3.3 The content of any School-sanctioned social media site and/or social media

accounts using the name of TMHS, a TMHS logo, or clearlyattached to TMHS in some way, should be entirely professional and should reflect well on the School.

3.3.4 Staff must not publish photographs of pupils without the written consent of parents / carers, or the pupil themselves if they are deemed of the age and ability to provide their own consent. Standard practice is to publish only the first name and initial of surname, unless permission has been given by parents or pupils (if deemed of the age and ability to provide their own consent) for the full name to be used. School sanctioned social media sites must use images of children in suitable clothing.

3.3.5 Staff must take into account the Safeguarding Policy when making any posts on school social media accounts.

3.3.6 Any links to external sites from the accounts must be appropriate and safe; if they are shared these must be verified as reputable sites. Only appropriate hashtags should ever be used.

3.3.7 Any inappropriate comments on, or abuse of, school-sanctioned social media and/or social media accounts using the name of TMHS, a TMHS logo, or clearly attached to TMHS in some way, should immediately be removed and reported to the Designated Safeguarding Lead (DSL) It is the responsibility of everyone using the site and social media in general to report abuse immediately.

3.3.8 All school sanctioned social media accounts created for school purposes should include a link in the About or Info page to this policy on the School website. This will indicate that the account is officially sanctioned by the School.

3.4 Use of social media in practice for staff - for personal and professional use

3.4.1 Staff must not have 1:1 communication, including direct messaging (DM), with pupils through any social media, apart from via school email accounts and school mobile devices for text messaging. 1:1 communication via Google Meet as part of the Schools OnlineLearning, must follow the School's Online Learning: Policy and Procedures for Teaching Staff.

3.4.2 Staff should not request or accept any current student of the School of any age or any ex-student of the School under the age of 18 as a friend, follower, subscriber or similar on any personal social media account unless they are the parent of the pupil or a close family member.

3.4.3 It is advisable that staff do not have contact with past pupils (above school age).

Staff may remain in communication with past pupils via a school email account or the School social media accounts.

3.4.4 Upper Sixth pupils are invited to join The Alumni, that staff are also members of, following the leavers' briefing.

3.4.5 Any communication received from current pupils on any personal social media sites must be reported immediately to the DSL.

3.4.6 If any member of staff is aware of any inappropriate communications involving any student in any social media, these must immediately be reported to the DSLs.

3.4.7 Members of staff must ensure that, wherever possible, and where the social media site allows, their privacy settings on social media sites are set so that pupils cannot access information relating to their personal lives or follow them ontheir personal accounts.

3.4.8 All email communication between staff and pupils of the School on school business must be made from an official school email account (any deviation from this in an emergency must at once be reported to the line manager). Staff should only use school mobile phones on trips or sports events and should not use personal email accounts or personal mobile phones to make contact with pupils of the School, nor should any such contact be accepted, except in circumstances such as school trips or away matches that have been given prior approval by the Headteacher. Prior approval may also be given by the Headteacher for staff to communicate professionally with pupils on School premises for safety reasons.

3.4.9 Staff should not post or publish on the internet or on any social networking site, any reference to the School, their colleagues, parents or pupils or discuss pupils or colleagues or criticise the School or staff. Staff may like, share or make appropriate comment in response to the School's official social media accounts,in accordance with Section 4.

3.4.10 Staff must not post images on any unofficial TMHS social media account that includes pupils, unless sharing posts made from a School official social media account.

3.4.11 Staff are instructed to consider the reputation of the School in any posts or comments related to the School on any social media accounts. Reputational breaches by staff are dealt with via the Disciplinary Policy.

3.4.12 Members of staff are responsible for overseeing and monitoring any social media account attributed to their area of responsibility where the social media account is

using the name of TMHS, a TMHS logo, or clearly attached to TMHS in some way.

3.5 Guidance and advice for staff

Most common social networking sites are inherently insecure places to have discussions which contain any sensitive information. Privacy laws can be violated, and the reputation of our school can be damaged if the public sees a discussion of any sensitive information taking place on social networking. Staff should be aware that these types of cases can resultin disciplinary action. Staff should refer to Teacher Standards Part 2: Personal and professional conduct for more information.

Proprietary Information

Staff may not share information which is confidential and proprietary about the School. This includes information about services, programmes, financial, strategy, and any other internal confidential, proprietary, or sensitive workplace information that has not been publicly released by the School. These are given as examples only and do not cover the range of what the School considers confidential and proprietary. If staff have any questions about whether information is proprietary, they must speak to their Line Manager or SMT member before releasing it. Staff must also be aware of the points made within their employment contract when they joined the School, a copy which can be obtained from the Headteacher's PA.

The School's logo and mascots may not be used without explicit permission in writing from SMT; the School owns the rights to all logos, mascots, mottos andphraseology and their usage.

Workplace Privacy

The School respects staff member rights to privacy and to express themselves. However, the School and staff members must also respect, and diligently protect, the privacy of fellow staff members, pupils, parents, and others. Privacy and confidentiality must be maintained inevery possible way.

Staff must not discuss pupil or family related information via social networking and public social media, texting, or online unless it is an approved medium and for a school related purpose.

Staff are advised to be extremely cautious in conversations with other staff, parents and volunteers in social networking, on the basis that privacy laws can be violated even if a person's name is not shared.

The School will honour the privacy rights of current and past employees, current and past pupils and their families, and anyone else associated with the School, by seeking permission before writing about or displaying internal school happenings which might be considered to be a breach of their privacy and confidentiality.

Privacy and Security Settings

The School recommends staff use security and privacy settings provided by social networking sites. Regardless of privacy settings, staff are advised to be respectful and responsible in all activity if it in

any way involves or references the School, job, or those staffwork with.

Staff must understand that on-line content is difficult, if not impossible to retract once posted or sent.

Blogging and Websites

If staff are developing a website or writing a blog that will mention the School and/or our Common Room, staff, Governors, pupils, parents and volunteers, they MUST get permissionfirst before writing anything, and advise the Headteacher they are intending to do this. The Headteacher may choose to inspect this from time to time.

It is important that staff make appropriate decisions about work-related blogging and the content of blogs, personal websites, postings on wikis and other interactive sites. Staff are advised to use caution with postings on video or picture-sharing sites, or in comments madeelsewhere on the public internet and in responding to comments from posters either publiclyor via email. If staff are assisting pupils to develop a website or blog, this must first be approved by the Headteacher and the Headteacher member must be given password access.

Legal Liability

Staff should recognise that there is the possibility of being legally liable for something inappropriate which is shared online.

The Media

If a member of the media or non-traditional online media (including bloggers) contacts a member of staff about the business of the School (e.g., programmes, services, pupils, parents, clubs, policies, practices, or additional business information of any kind), the individual must contact the Headteacher prior to responding.

3.6 Use of social media in practice for pupils

3.6.1 Pupils use of social media on any School IT systems, School Managed Chromebooks and School IT accounts accessed at any time (including during online learning) and equipment/devices and any personal devices (including hand held devices, watches or any other internet enabled device) brought on to the School site or at a School activity, must comply with the Pupils'Computer/Device Usage Agreement and the School's Online Safety and ICT Acceptable Use Policy. Pupils should also follow any additional code of conduct /guidelines put in place for online learning from home.

3.6.2 Pupils must not access any social media that is for adults only or if the pupil does not meet the minimum age requirement.

3.6.3 Anonymous sites must not be accessed as there is a high risk that inappropriate

comments can be exchanged, causing distress or endangerment.

3.6.4 Bad, including offensive, explicit or abusive, language and inappropriate pictures must never be included in messages.

3.6.5 All messages should be positive and not include anything that could be upsetting or defamatory towards others or the School.

3.6.6 Pupils must take responsibility for keeping details of their accounts private, using full privacy settings and logging off properly and not allowing others to use their accounts.

3.6.7 Pupils must report anything offensive or upsetting that they see online to the appropriate bodies, either by using the "report abuse" tabs or by speaking to their parents or a member of staff.

3.6.8 It is a serious offence to use another person's account, or to create an account in another person's name without their consent.

3.6.9 Pupils should not regard anything posted online as private and should remember that harassment, defamatory attitudes and racism are just some issues which could lead to prosecution.

3.6.10 An individual's "Digital Footprint" is becoming increasingly significant when it comes to job and university applications. If unfortunate decisions are made, it will be extremely difficult, perhaps impossible, to eliminate the evidence.

3.6.11 If pupils see inappropriate postings by other pupils, they must inform the school so that steps can be taken to avoid possible repercussions.

3.6.12 The Malicious Communications Act applies to social media interaction by Pupils, Staff and Parents of the School.

3.6.13 Pupils must have permission from the relevant Head of Department for any social media accounts using the name of TMHS, a TMHS logo, or clearly attached to TMHS in some way

3.7 Use of social media in practice for parents

3.7.1 Positive contributions to the School Social Media, such as Twitter, are welcomed.

3.7.2 Any concerns or issues about the School, its pupils or staff should be expressed directly to the School and not be voiced on social media.

3.7.3 Parents must obtain permission before posting pictures that contain other parents or their children, unless sharing or liking a post from the School's official social media account.

3.7.4 If parents become aware of inappropriate use of social media by their own or other people's children, they should contact the School so that the School can work with the parents to educate young people on safe and appropriate behaviour.

3.7.5 If parents become aware of the inappropriate use of social media by other parents or school staff, they should inform the School so that steps can be takento remedy the situation.

Further Guidance

Further guidance on educating and safeguarding young people online and responding to incidents:

Sexting
UK Council for Child Internet Safety Guidance - Sexting

Online safety advice for pupils, parents and teachers:
www.thinkuknow.co.uk
http://www.saferinternet.org.uk
/
https://www.internetmatters.org
/

Cyberbullying
www.childnet.com/cyberbullying-guidance

Preventing radicalisation
educateagainsthate.com

www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

Social Media Restrictions for Social Media Platforms

What are the age limits for social media apps and platforms?

It is vital that parents, pupils and staff know the age restrictions that are applied to manypopular apps. As this is a fast-moving area, we would recommend that parents (with their child) always check before a child accesses an app from an internet safety website such asInternet Matters, for which there is a link below. We do not endorse the use of these apps; this information is provided

only to help support your children to use social media safely.

https://www.internetmatters.org/resources/what-age-can-my-child-start-social-networking/

4. Cyber Security

4.1 Types of security breach and causes

Unauthorised use without damage to data – involves unauthorised persons accessing data on the school system, e.g. 'hackers', who may read the data or copy it, but who do not actually damage the data in terms of altering or deleting it. This includes unauthorised people within the school, e.g. schools where pupils access systems that staff have left open and/or logged in, or where staff access data beyond their authorisation, as can occur in schools where all staff are given admin-level access for ease.

Unauthorised removal of data – involves an authorised person accessing data, who removes the data to pass it on to another person who is not authorised to view it, e.g. a staff member with authorised access who passes the data on to a friend without authorised access. This is also known as data theft. The data may be forwarded or deleted altogether.

Damage to physical systems – involves damage to the hardware in the school's ICT system, which may result in data being inaccessible to the school and/or becoming accessible to unauthorised persons.

Unauthorised damage to data – involves an unauthorised person causing damage to data, either by altering or deleting it. Data may also be damaged by a virus attack, rather than a specific individual.

Breaches in security may be caused by the actions of individuals, and may be accidental, malicious or the result of negligence:

- Accidental breaches can occur as a result of human error or insufficient training for staff, so they are unaware of the procedures to follow
- Malicious breaches can occur as a result of a hacker wishing to cause damage to the school through accessing and altering, sharing or removing data

Breaches caused by negligence can occur as a result of a staff member knowingly disregarding school policies and procedures or allowing pupils to access data without authorisation and/or supervision

Breaches in security may also be caused by system issues, which could involve incorrect installation, configuration problems or operational errors:

- The incorrect installation of antivirus software and/or use of outdated software can make the school software more vulnerable to a virus
- Incorrect firewall settings being applied, e.g. unrestricted access to the school network, can allow unauthorised individuals to access the school system
- Operational errors, such as confusion between back-up copies of data, can cause the most recent data to be overwritten

Roles and responsibilities

The governing board will be responsible for:

- Ensuring the school has appropriate cyber-security measures in place.
- Ensuring the school has an appropriate approach to managing data breaches in place.
- Supporting the headteacher and other relevant staff in the delivery of this policy.
- Ensuring the school meets the relevant cyber-security standards.

The headteacher will be responsible for:

- Ensuring all staff members and pupils are aware of their responsibilities in relation to this policy.
- Ensuring appropriate user access procedures are in place.
- Responding to alerts for access to inappropriate content in line with the Online Safety Policy.
- Organising training for staff members in conjunction with the online safety officer and DPO.
- Ensuring a log of cyber-security incidents is maintained.
- Appointing a cyber recovery team who is responsible for implementing the school's procedures in the event of a cyber-security incident.

The DPO will be responsible for:

- The overall monitoring and management of data security.
- Deciding which strategies are required for managing the risks posed by internet use.
- Leading on the school's response to incidents of data security breaches, including leading the cyber recovery team.
- Assessing the risks to the school in the event of a cyber-security breach.
- Determining which organisations and individuals need to be notified following a data security breach, and ensuring they are notified.
- Working with the ICT technician, online safety officer and headteacher after a data security breach to determine where weaknesses lie and improve security measures.
- Organising training for staff members on data security, network security and preventing breaches.
- Monitoring and reviewing the effectiveness of this policy, alongside the headteacher, and communicating any changes to staff members.

The ICT manager will be responsible for:

- Maintaining an inventory of all ICT hardware and software currently in use at the school.
- Ensuring any out-of-date software is removed from the school systems.
- Implementing effective firewalls to enhance network security and ensuring that these are monitored regularly.
- Installing, monitoring and reviewing filtering systems for the school network.
- Setting up user privileges in line with recommendations from the headteacher.
- Maintaining an up-to-date and secure inventory of all usernames and passwords.
- Removing any inactive users from the school system and ensuring that this is always up-to-date.

- Installing appropriate security software on staff members' personal devices where the headteacher has permitted for them to be used for work purposes.
- Performing a back-up of all electronic data held by the school, ensuring detailed records of findings are kept.
- Ensuring all school-owned devices have secure malware protection and are regularly updated.
- Recording any alerts for access to inappropriate content and notifying the headteacher.

The online safety officer will be responsible for:

- Organising training and resources for staff on online safeguarding risks and preventative measures.
- Taking responsibility for online safety within the school and promoting online safety measures to parents.
- Ensuring the relevant policies and procedures are in place to protect pupils from harm, including the Online Safety Policy.
- Monitoring online safety incidents which could result in data breaches and reporting these to the DPO.
- Acting as the named point of contact within the school on all online safety issues.
- Liaising with relevant members of staff on online safety matters, e.g. the DPO and ICT Department.

The DSL will be responsible for:

- Assessing whether there is a safeguarding aspect to any cyber-security incident and considering whether any referrals need to be made.

All staff members will be responsible for:

- Understanding their responsibilities in regard to this policy.
- Undertaking the appropriate training.
- Ensuring they are aware of when new updates become available and how to safely install them.

4.2 Secure configuration

An inventory will be kept of all ICT hardware and software currently in use at the school, including mobile phones and other personal devices provided by the school. The inventory will be stored in the **school office** and will be audited on a **termly** basis to ensure it is up-to-date. Any changes to the ICT hardware or software will be documented using the inventory and will be authorised by the ICT technician before use.

All systems will be audited on a **termly** basis by the ICT manager to ensure the software is up-to-date. Any new versions of software or new security patches will be added to systems, ensuring that they do not affect network security, and will be recorded in the inventory. Any software that is out-of-date or reaches its 'end of life' will be removed from systems, e.g. when suppliers end their support for outdated products, meaning that the product is not able to fulfil its purpose anymore.

All hardware, software and operating systems will require passwords from individual users. The school believes that locking down hardware, such as through the use of strong passwords, is an effective way to prevent access to facilities by unauthorised users. Passwords will need to adhere to a specific character length, use special characters, and not be obvious or easy to guess, in line with the school's policy on passwords.

The school will consider referring to the five security controls outlined in the National Cyber Security Centre's (NCSC's) 'Cyber Essentials'. These are:

- **Firewalls** – Firewalls function as a barrier between internal networks and the internet. They will be installed on any device that can access the internet, particularly where staff are using public or otherwise insecure Wi-Fi.
- **Secure configuration** – The default configurations on devices and software are often as open as possible to ensure ease of use, but they also provide more access points for unauthorised users. The school will disable or remove any unnecessary functions and change default passwords to reduce the risk of a security breach.
- **Access control** – The more people have access to data, the larger the chance of a security breach. The school will ensure that access is given on a 'need-to-know' basis to help protect data. All accounts will be protected with strong passwords, and where necessary, two-factor authorisation.
- **Malware protection** – The school will protect itself from malware by installing antivirus and anti-malware software, and using techniques such as whitelisting (a cyber-security strategy under which a user can only take actions on their computer that an administrator has explicitly allowed in advance) and sandboxes (an isolated virtual machine in which potentially unsafe software code can execute without affecting network resources or local applications).
- **Patch management** – The school will install software updates as soon as they are available to minimise the time frame in which vulnerabilities can be exploited. If the manufacturer stops offering support for the software, the school will replace it with a more up-to-date alternative.

The ICT manager will:

- Protect every device with a correctly configured boundary, or software firewall, or a device that performs the same function.
- Protect access to the firewall's administrative interface with multi-factor authentication (MFA), or a small, specified IP-allow list combined with a managed password, or prevent access from the internet entirely.
- Keep firewall firmware up to date.
- Check monitoring logs as they can be useful in detecting suspicious activity.
- Block inbound unauthenticated connections by default.
- Document reasons why particular inbound traffic has been permitted through the firewall.
- Review reasons why particular inbound traffic has been permitted through the firewall often, change the rules when access is no longer needed.
- Enable a software firewall for devices used on untrusted networks, like public wi-fi.

All devices will be set up in a way that meets the standards described in the technical requirements.

The ICT manager will devise a system for monitoring logs and documenting decisions made on inbound traffic.

4.3 Network security

In line with the UK GDPR, the school will appropriately test, assess, and evaluate any security measures put in place on a **termly** basis to ensure these measures remain effective.

The school will employ firewalls in order to prevent unauthorised access to the systems.

Localised firewall deployment

The school's firewall will be deployed as a localised deployment, which means the broadband service connects to a firewall that is located on an appliance or system on the school premises, as either discrete technology or a component of another system.

As the school's firewall is managed on the premises, it is the responsibility of the ICT technician to effectively manage the firewall. The ICT technician will ensure that:

- The firewall is checked **weekly** for any changes and/or updates, and that these are recorded using the inventory.
- Any changes and/or updates that are added to servers, including access to new services and applications, are checked to ensure that they do not compromise the overall network security.
- The firewall is also checked **weekly** to ensure that a high level of security is maintained, and there is effective protection from external threats.
- Any compromise of security through the firewall is recorded using an incident log and is reported to the DPO. The ICT technician will react appropriately to security threats to find new ways of managing the firewall.

The school will be aware that security standards may change over time with changing cyber threats.

The school will ensure that the security of every device on its network is reviewed regularly.

The school will agree with the ICT manager a system for recording and reviewing decisions made about network security features.

To ensure that the network is as secure as possible, the school will:

- Keep a register, list, or diagram of all the network devices.
- Avoid leaving network devices in unlocked or unattended locations.
- Remove or disable unused user accounts, including guest and unused administrator accounts.
- Change default device passwords.
- Require authentication for users to access sensitive school data or network data.
- Remove or disable all unnecessary software according to your organisational need.

- Disable any auto-run features that allow file execution.
- Set up filtering and monitoring services to work with the network's security features enabled.
- Immediately change passwords which have been compromised or suspected of compromise.
- Protect against a brute-force attack on all passwords by allowing no more than 10 guesses in five minutes, or locking devices after no more than 10 unsuccessful attempts.

Unlicensed hardware or software will never be used by the school.

All unpatched or unsupported hardware or software will be replaced by the ICT Dept. Where it is not possible to replace these devices, they will have their access to the internet removed so that scanning tools cannot find weaknesses.

4.4 Malware prevention

The school understands that malware can be damaging for network security and may enter the network through a variety of means, such as email attachments, social media, malicious websites or removable media controls.

The ICT Dept will ensure that all school devices have secure malware protection and undergo regular malware scans in line with specific requirements. The ICT Dept will update malware protection on a regular basis to ensure it is up-to-date and can react to changing threats. Malware protection will also be updated in the event of any attacks to the school's hardware and software.

Filtering of websites, as detailed in the 'User privileges and passwords' section of this policy, will ensure that access to websites with known malware are blocked immediately and reported to the ICT Dept.

The school will use mail security technology, which will detect and block any malware that is transmitted by email. This will also detect any spam or other messages which are designed to exploit users. The ICT Dept will review the mail security technology on a regular basis to ensure it is kept up-to-date and effective.

Staff members are only permitted to download apps on any school-owned device from manufacturer-approved stores and with prior approval from the online safety officer. Where apps are installed, the ICT Dept will keep up-to-date with any updates, ensuring staff are informed of when updates are ready and how to install them.

The school will use anti-malware software that:

- Is set up to scan files upon access, when downloaded, opened, or accessed from a network folder.
- Scans web pages as they are accessed.
- Prevents access to potentially malicious websites, unless risk-assessed, authorised and documented against a specific business requirement.

4.5 User privileges and passwords

The school understands that controlling what users have access to is important for promoting network security and data protection. User privileges will be differentiated, e.g. pupils will have different access to data and the network than members of staff, whose access will also be role-based.

The headteacher will clearly define what users have access to and will communicate this to the ICT Dept, ensuring that a written record is kept. The ICT Dept will ensure that user accounts are set up to allow users access to the facilities required, in line with the headteacher's instructions, whilst minimising the potential for deliberate or accidental attacks on the network.

All users will be required to change their passwords if they become known to other individuals, in line with the 'Secure configuration' section of this policy. Pupils are responsible for remembering their passwords; however, the ICT Dept will have an up-to-date record of all usernames and will be able to reset passwords if necessary. Multi-factor authentication (multiple different methods of verifying the user's identity) should be used wherever possible.

A multi-user account will be created for visitors to the school, such as volunteers, and access will be filtered as per the headteacher's instructions. Usernames and passwords for this account will be changed on a regular basis and will be provided as required.

Automated user provisioning systems will be employed in order to automatically delete inactive users or users who have left the school. The ICT Dept will manage this provision to ensure that all users that should be deleted are, and that they do not have access to the system.

Password strength will be enforced at a system level – the school will use a deny list for automatic blocking of common passwords and passwords must contain a minimum of eight characters.

The school will implement a user account creation, approval and removal process which is part of the school joining and leaving protocols.

User accounts and access privileges will be appropriately controlled, and only authorised individuals will have an account which enables them to access, alter, disclose or delete personal data.

Users (Except ICT Dept) will have a separate account for routine business if their main account:

- Is an administrative account.
- Enables the execution of software that makes significant system or security changes.
- Can make changes to the operating system.
- Can create new accounts.
- Can change the privileges of existing accounts.

The school will consider using multi-factor authentication, particularly for accounts that have access to sensitive or personal data.

The ICT Dept will review the password system on a regular basis to ensure it is working at the required level.

4.6 Monitoring usage

Monitoring user activity is important for the early detection of attacks and incidents, as well as inappropriate usage by pupils or staff. The school will inform all pupils and staff that their usage will be monitored, as well as how it is being monitored and why, in accordance with the school's Online Safety Policy.

If a user accesses inappropriate content or a threat is detected, an alert will be sent to the Safeguarding Leads and the ICT Dept. Alerts will also be sent for unauthorised and accidental access. Alerts will identify the user, the activity that prompted the alert, and the information or service the user was attempting to access.

The ICT Dept will record any alerts using an incident log and will report this to the DPO. The DPO will then inform the headteacher and online safety officer as appropriate. All incidents will be responded to in accordance with the 'Data security breach incidents' section of this policy, and as outlined in the Online Safety Policy.

The ICT Dept will ensure that websites are filtered on a regular basis for inappropriate and malicious content. Any member of staff or pupil that accesses inappropriate or malicious content will be recorded in accordance with the monitoring process in the 'Data security breach incidents' section of this policy.

All data gathered by monitoring usage will be kept for easy access when required. This data may be used as a method of evidence for supporting a not-yet-discovered breach of network security. In addition, the data may be used to ensure the school is protected and all software is up-to-date.

4.7 Removable media controls

The school understands that pupils and staff may need to access the school network from outside the school premises. Effective security management will be established to prevent access to, or leakage of, data, as well as any possible risk of malware.

The ICT Dept will encrypt all data storage devices for personal use, such as USB sticks, to ensure that they are password protected. If any portable devices are lost, this will prevent unauthorised access to personal data.

Before distributing any school-owned devices, the ICT Dept will ensure that manufacturers' default passwords have been changed. A set password will be chosen, and the staff member will be prompted to change the password once using the device. The ICT Dept will check school-owned devices on a regular basis to detect any unchanged default passwords.

When using laptops, tablets and other portable devices, the headteacher will determine the limitations for access to the network, as described in the 'Network security' section of this policy.

Staff who use school-owned laptops, tablets and other portable devices will use them for work purposes only, whether on or off the school premises. Staff will avoid connecting to unknown Wi-Fi hotspots, such as in coffee shops, when using any school-owned laptops, tablets or other devices, or when accessing school networks.

The online safety officer will use encryption to filter the use of websites on school-owned devices in order to prevent inappropriate use and external threats which may compromise network security when bringing the device back onto the premises. The school uses tracking technology where possible to ensure that lost or stolen school-owned devices can be retrieved.

All data will be held on systems centrally in order to reduce the need for the creation of multiple copies, and/or the need to transfer data using removable media controls.

The Wi-Fi network at the school will be password protected and will only be given out as required. Staff and pupils are not permitted to use the Wi-Fi for their personal devices, such as mobile phones or tablets, unless agreed prior to usage. A separate Wi-Fi network will be established for visitors at the school to limit their access to school networks and any other applications which it is not necessary for them to access.

4.8 Home working and remote learning

Staff and pupils will adhere to data protection legislation and the school's related policies when working remotely.

Staff will receive training regarding what to do if a data protection issue arises from any home working or remote learning.

Wherever possible, personal data will not be taken home by staff members for the purposes of home working, due to the risk of data being lost or the occurrence of a data breach.

Staff and pupils may be required to use their own devices for the duration of the remote working or learning period. Any user on a personal device will need to access the school system through a proxy, e.g. VPN. Using a shared personal or household device for school purposes should be avoided where possible; however, the school understands that this may not always be possible.

Staff and pupils are not permitted to let their family members or friends use any school equipment, in order to protect the confidentiality of any personal data held on the device. Any staff member found to have shared personal data without authorisation will be disciplined in line with the Disciplinary Policy and Procedure. This may also result in a data breach that the school would need to record and potentially report to the ICO.

Staff who require access to personal data to enable them to work from home will first seek approval from the headteacher, and it will be ensured that the appropriate security measures are in place by the ICT Dept and the DPO, e.g. secure passwords and anti-virus software.

Staff will be informed that caution should be exercised while accessing personal data if an unauthorised person is in the same room. If a member of staff needs to leave their device unattended, the device should be locked. School devices will automatically lock after a period of inactivity to avoid an unauthorised person gaining access to the device. Where staff are using a personal device, they will be advised that a similar function should be implemented.

Personal data should only be transferred to a home device if this is necessary for the member of staff to carry out their role. When sending confidential information, staff must never save confidential information to a personal or household device. Data that is transferred from a work to a home device

will be encrypted so that if any data is lost, stolen or subject to unauthorised access, it will remain safe until it can be recovered.

To ensure reasonable precautions are taken when managing data, staff will avoid:

- Keeping personal data on unencrypted hard drives.
- Sending work emails to and from personal email addresses.
- Leaving logged-in devices and files unattended.
- Using shared home devices where other household members can access personal data.
- Using an unsecured Wi-Fi network.

Staff working from home will be encouraged and enabled to go paperless, where possible, as paper files cannot be protected digitally and may be misplaced. If sensitive data is taken off the school premises to allow staff to work from home, it will be transported in a lockable bag or container. The school's procedures for taking data off the school premises will apply to both paper-based and electronic data.

When taking physical copies of data, e.g. paper documents and school-owned devices, off the school premises, staff will sign out the documents with the Business Manager or HTPA. The physical data will be signed back in when staff return it.

Pupils are not permitted to use school-owned devices or software for activities that do not pertain to their online education, e.g. use of social media, gaming, streaming or viewing content that is not applicable to their curriculum. Pupils are not permitted to download any software onto school devices, unless instructed to and approved by their teacher.

Pupils will not alter the passwords or encryptions protecting school documents and systems put in place by the school. Pupils will not alter or disable any security measures that are installed on school devices, e.g. firewalls, malware prevention or anti-virus software. Pupils will not share any confidential and/or personal information made accessible to them, e.g. VPN passwords, with anyone who is not authorised to view that information.

Pupils that do not use school devices or software in accordance with this policy will be disciplined in line with the Behavioural Policy.

Pupils must report any technical issues to their teacher as soon as possible. Parents and pupils will be encouraged to contact the online safety officer if they wish to report any concerns regarding online safety.

Any devices that are used by staff and pupils for remote working and learning will be assessed by the ICT dept prior to being taken to the home setting, using the following checks:

- System security check – the security of the network and information systems
- Data security check – the security of the data held within the systems
- Online security check – the security of any online service or system, e.g. the school website
- Device security check – the security of the personal device, including any 'bring your own device' systems

The ICT Dept will provide staff and pupils with details and instructions for accessing the school network that they will be using throughout the duration of the remote working and learning period.

In the event that a staff member or pupil decides to leave the school permanently, all data in any form will be returned on or before their last day.

4.9 Backing up data

The ICT Dept performs a back-up of all electronic data held by the school on a termly basis, and the date of the back-up is recorded using a log. Each back-up is retained for up to 90 days before being deleted. The ICT Dept performs an incremental back-up on a nightly basis of any data that has changed since the previous back-up. The ICT Dept will record the date of any incremental back-up, alongside a list of the files that have been included in the back-up.

The ICT Dept will ensure that there are at least three backup copies of important data, on at least two separate devices – one of which will remain off-site, e.g. tape backups.

The number of devices with access to back up data will be kept to an absolute minimum.

The school must follow the NCSC's guidance on backing up data where necessary, including:

- Identifying what essential data needs to be backed up.
- Storing backed-up data in a separate location to the original data.
- Considering using the Cloud to store backed-up data.
- Referring to the NCSC's Cloud Security Guidance.
- Ensuring that backing up data is regularly practised.

Where possible, back-ups are run overnight and are completed before the beginning of the next school day. Upon completion of back-ups, data is stored on the school's hardware, which is password protected. Data will be replicated and stored in accordance with the school's Data Protection Policy. Only authorised personnel will be able to access back-ups of the school's data.

The school will ensure that offline or 'cold' back-ups are secured. This can be done by only digitally connecting the back-up to live systems when necessary, and never having all offline back-ups connected at the same time.

The school's back-up strategy will be tested on a regular basis.

4.10 Avoiding phishing attacks

The ICT Dept will configure all staff accounts using the principle of 'least privilege' – staff members are only provided with as much rights as are required to perform their jobs.

Staff will use the following warning signs when considering whether a communication may be unusual:

- Is it from overseas?
- Is the spelling, grammar and punctuation poor?
- Is the design and quality what you would expect from a large organisation?
- Is it addressed to a 'valued customer', 'friend' or 'colleague'?

- Does it contain a veiled threat that asks the staff member to act urgently?
- Is it from a senior member of the school asking for a payment?
- Is it from a supplier advising of a change in bank account details for payment?
- Does it sound too good to be true? It is unlikely someone will want to give another individual money or access to another service for free.
- Is it from a generic email address, such as Gmail or Hotmail?

The ICT Dept will ensure that an appropriate email filtering system is used to identify which emails would be classed as junk or spam, applied in accordance with the 'Malware prevention' section of this policy. The ICT Dept will ensure that the filtering system is neither too strict nor too lenient, to allow the correct emails to be sent to the relevant folders.

To prevent anyone having access to unnecessary personal information, the DPO will ensure the school's social media accounts and websites are reviewed on a regular basis, making sure that only necessary information is shared. The headteacher and DPO will ensure the school's Social Media Policy includes expectations for sharing of information and determines what is and is not appropriate to share.

The headteacher will ensure parents, pupils, staff and other members of the school community are aware of acceptable use of social media and the information they share about the school and themselves.

4.11 User training and awareness

The DPO and headteacher will arrange training for pupils and staff on a regular basis to ensure they are aware of how to use the network appropriately. This will cover identifying irregular methods of communication in order to help staff members spot requests that are out of the ordinary, such as receiving an invoice for a service not used, and who to contact if they notice anything unusual. Unusual communications could come in a variety of forms, e.g. emails, phone calls, text messages or social media messages.

The online safety officer will arrange for staff and pupils to undertake the appropriate training relating to online safety issues.

The DPO will also arrange training for pupils and staff on a regular basis on maintaining data security, preventing data breaches, and how to respond in the event of a data breach. Training for all staff members will be arranged by the online safety officer and DPO within **two weeks** following an attack, breach or significant update.

Through training, all pupils and staff will be aware of who they should inform first in the event that they suspect a security breach, and who they should inform if they suspect someone else is using their passwords. All staff will receive training as part of their induction programme. All pupils will receive training upon joining the school.

All users will be made aware of the disciplinary procedures for the misuse of the network leading to malicious attacks, in accordance with the process detailed in the Behavioural Policy and the Disciplinary Policy and Procedure.

4.12 Cyber-security incidents

All cyber-security incidents will be managed in line with the school's Cyber Response and Recovery Plan.

Any individual that discovers a cyber-security incident will report this immediately to the headteacher and the DPO.

When an incident is raised, the DPO will record the following information:

- Name of the individual who has raised the incident
- Description and date of the incident
- Description of any perceived impact
- Description and identification codes of any devices involved, e.g. school-owned laptop
- Location of the equipment involved
- Contact details for the individual who discovered the incident
- Whether the incident needs to be reported to the relevant authorities, e.g. the ICO or police

The school's DPO will take the lead in investigating the incident, with assistance from the cyber recovery team, and will be allocated the appropriate time and resources to conduct this. The DPO, as quickly as reasonably possible, will ascertain the severity of the incident and determine if any personal data is involved or has been compromised. The DPO will oversee a full investigation and produce a comprehensive report. The cause of the incident, and whether it has been contained, will be identified – ensuring that the possibility of further loss or jeopardising of data is eliminated or restricted as much as possible.

If the DPO determines that the severity of the security breach is low, the incident will be managed in accordance with the following procedures:

- In the event of an internal breach, the incident is recorded using an incident log, and by identifying the user and the website or service they were trying to access
- The headteacher will issue disciplinary sanctions to the pupil or member of staff who caused the breach, in accordance with the Behavioural Policy or Disciplinary Policy and Procedure
- In the event of any external or internal breach, the DPO will record this using an incident log and respond appropriately, e.g. by updating the firewall, changing usernames and passwords, updating filtered websites or creating further back-ups of information
- The school will organise updated staff training following a breach
- Any further action which could be taken to recover lost or damaged data will be identified – this includes the physical recovery of data, as well as the use of back-ups

Where the security risk is high, the DPO will establish what steps need to be taken to prevent further data loss, which will require support from various school departments and staff. This action will include:

- Informing relevant staff of their roles and responsibilities in areas of the containment process.
- Taking systems offline.
- Retrieving any lost, stolen or otherwise unaccounted for data.

- Restricting access to systems entirely or to a small group.
- Backing up all existing data and storing it in a safe location.
- Reviewing basic security, including:
    - Changing passwords and login details on electronic equipment.
    - Ensuring access to places where electronic or hard data is kept is monitored and requires authorisation.

Where appropriate, e.g. if offences have been committed under the Computer Misuse Act 1990, the DPO will inform the police of the security breach.

Schools are required to report personal data breaches to the ICO if there is a likelihood of risk to people's rights and freedoms. If the DPO decides that risk is unlikely, the breach does not need to be reported; however, the school will need to justify this decision and document the breach.

The DPO will notify the ICO within 72 hours of becoming aware of a breach where it is likely to result in a risk to the rights and freedoms of individuals.

The UK GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours. The information required can be provided in phases, as long as this is done without undue further delay.

In line with the UK GDPR, the following must be provided to the ICO when reporting a personal data breach:

- A description of the nature of the breach, including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the breach
- A description of the measures taken, or proposed to be taken, to deal with the breach
- A description of the measures taken to mitigate any possible adverse effects, where appropriate

The school will report a personal data breach via the ICO website. The school will also make use of the ICO's self-assessment tool to determine whether reporting a breach is a necessary next step.

Where a breach is likely to result in a significant risk to the rights and freedoms of individuals, the DPO will notify those concerned directly of the breach without undue delay.

Where the school has been subject to online fraud, scams or extortion, the DPO will also report this using the Action Fraud website.

The DPO and ICT Dept will test all systems to ensure they are functioning normally, and the incident will only be deemed 'resolved' when it has been assured that the school's systems are safe to use.

The trust is aware it must seek permission from the ESFA to pay any cyber-ransom demands in the event of a cyber-crime.

4.13 Assessment of risks

The following questions will be considered by the DPO to fully and effectively assess the risks that the cyber-security breach has brought, and to help take the next appropriate steps. All relevant questions will be clearly and fully answered in the DPO's report, which should record:

- What type of, and how much, data is involved?
- How sensitive is the data? Sensitive data is defined in the UK GDPR; some data is sensitive because of its very personal nature (e.g. health records) while other data types are sensitive because of what might happen if it is misused (e.g. bank account details).
- Is it possible to identify what has happened to the data – has it been lost, stolen, deleted or tampered with?
- If the data has been lost or stolen, were there any protective measures in place to prevent this, such as data and device encryption?
- If the data has been compromised, have there been effective measures in place that have mitigated the impact of this, such as the creation of back-up tapes and spare copies?
- Has individuals' personal data been compromised – how many individuals are affected?
- Who are these individuals – are they pupils, staff, governors, volunteers, stakeholders, suppliers?
- Could their information be misused or manipulated in any way?
- Could harm come to individuals? This could include risks to the following:
    - Physical safety
    - Emotional wellbeing
    - Reputation
    - Finances
    - Identity
    - Private affairs becoming public
- Are there further implications beyond the risks to individuals? Is there a risk of loss of public confidence and/or damage to the school's reputation, or risk to the school's operations?
- Who could help or advise the school on the breach? Could the LA, external partners, authorities, or others provide effective support?
- Does the breach need to be reported to the ICO? If so, has it been successfully reported without undue delay?

In the event that the DPO, or other persons involved in assessing the risks to the school, are not confident in the assessment of risk, they will seek advice from the ICO.

4.14 Consideration of further notification

The DPO will consider whether there are any legal, contractual or regulatory requirements to notify individuals or organisations that may be affected or who will have an interest in data security.

The DPO will assess whether notification could help the individual(s) affected, and whether the individual(s) could act on the information provided to mitigate risks, e.g. by cancelling a credit card or changing a password. In line with the 'Data security breach incidents' section of this policy, if a large number of people are affected, or there are very serious consequences, the ICO will be informed.

The DPO will consider who to notify, what to tell them and how they will communicate the message, which may include:

- A description of how and when the breach occurred and what data was involved.
- Details of what has already been done to respond to the risks posed by the breach.
- Specific and clear advice on the steps they can take to protect themselves, and what the school is willing to do to help them.
- A way in which they can contact the school for further information or to ask questions about what has occurred.

The DPO will consider, as necessary, the need to notify any third parties, such as the police, insurers, professional bodies, funders, trade unions, website and/or system owners, banks and/or credit card companies, who can assist in helping or mitigating the impact on individuals.

4.15 Evaluation

The DPO will document all the facts regarding the breach, its effects and the remedial action taken. This should be an evaluation of the breach, and what actions need to be taken forward.

The DPO will consider the data and contexts involved, establish the root of the breach, and where any present or future risks lie, taking into consideration whether the breach is a result of human or systematic error and see how a recurrence can be prevented.

The DPO and headteacher will identify any weak points in existing security measures and procedures. The DPO will work with the ICT technician to improve security procedures wherever required. The DPO and headteacher will identify any weak points in levels of security awareness and training.

The DPO will report on findings and implement the recommendations of the report after analysis and discussion.

5. Guidance for staff on use of E-mail/Online conduct

Email is accepted as one of the primary methods of communication used in school on a daily basis. Email may even be the best way to communicate a particular message, but in an age of digital information 'overload', all staff should be mindful of the impact of an excessively email driven culture and make smart choices about what, when and how to communicate with others.
With many individuals now accessing emails across multiple personal and work devices, it is increasingly important to use email appropriately in a way that fosters professionalism and effectiveness whilst enabling staff to manage a reasonable work life balance.
It is also important that staff are aware of how best to use emails to enhance instead of hinder working practices and relationships with others.
Staff should be mindful of the principles and practice in this policy when using other online facilities such as chat functions and social media.

5.1 Guidance aims

5.1.1 This guidance covers all staff and sets out what is considered acceptable behaviour in relation to the use of emails between staff and others. This includes colleagues, parents, volunteers, trustees, contractors and other agencies.

5.1.2 This guidance focuses on email behaviour and etiquette and does not attempt to outline the technical requirements of email usage or other online facilities.

5.2 Guidance principles

5.2.1 Email communication is highly beneficial for speed, minimal cost and convenience. They are a formal written form or communication which is covered by a number of laws in the UK, meaning they can be used for legal purposes (e.g. an employment tribunal or court of law as evidence where it is deemed necessary).

5.2.2 Although it is often regarded as such, email should not be considered an informal method of speaking with others when dealing with School business, despite it being a fast and easy way of communicating. It is also important that it is recognised by all staff that intensive or overuse of email can result in negatively impacting recipients in a number of ways.

5.2.3 Excessive or inappropriate use of email, or emails with an excessive amount unnecessary content, can result in 'information overload', where an individual feels overwhelmed by the volume of emails received. This can lead to a number of negative outcomes such as stress, anxiety, miscommunication, indecision or poor decision making, procrastination and other counter-productive avoidance behaviours, though this is not an exhaustive list.

5.2.4 Staff should use their school accounts when administering or communicating school business. These accounts are not for personal use. Equally staff should not use personal email accounts for school business.

5.3 Fostering good working relationships

5.3.1 When sending emails, senders should be aware of their audience at all times.

5.3.2 What one may consider a reasonable tone may easily cause offence to another. Staff should ensure that care and attention is taken with email correspondence, just as it would be with a written letter, to reduce the chance of misinterpretation and misunderstanding.

5.3.3 The 'bcc' option should generally not be used in the interest of disclosure and full transparency of communications to all parties, both the sender and recipient.

5.3.4 If staff are receiving a high frequency of emails from one individual; or are receiving inappropriate emails they should seek advice from a member of SMT

5.4 Emails out of hours

5.4.1 One way of fostering good working relationships is being conscious of email use out of hours.

5.4.2 Owing to the nature of some roles at the School, and the range of locations these may be undertaken, emails sent outside school opening times will sometimes be both normal and

necessary. For many other roles across the School, out of hours emails should be the exception rather than the rule.

5.4.3 Emails sent outside of working hours can alleviate the sender's workload, particularly as teaching loads and/or other intensive periods of meetings and commitments are predominantly set within working hours or can be convenient where travel is required. With technology allowing staff to access emails via mobiles, tablet and laptops while on the move, the boundary between professional and personal arenas can also become increasingly blurred. Senders should consider the use of 'scheduled send' when working outside of working hours.

5.4.4 Whilst it is the prerogative of the sender to send an email whenever they choose, it is also the recipient's prerogative to choose when to read their incoming emails (i.e. normally within working hours), provided this is in line with the accepted levels of professional behaviour and aligned with the expectations of their role responsibilities. There should be no general expectation that staff will read emails out of hours. It is also advised where an urgent response is needed, a follow up by telephone may be more appropriate rather than a "chaser" email.

5.4.5 Senders should also be mindful of the impact on others when sending lots of emails out of hours, even if the sender does not expect a swift response. Arriving to work to a full "inbox" unexpectedly can be a stressor to recipients who may be deluged by emails both inside and outside of working hours.

5.4.6 During short or prolonged periods of School Closure, staff should still check emails as important information can be given.

5.5 Email communication with Parents

5.5.1 Email can be a useful form of communication with parents. In many cases Heads of Department, Heads of Years, Subject Teachers and Tutors may email directly. In other cases, parents may send an email to 'inmail' and a member of staff will be allocated to deal with the query. If you are unsure about how to respond to a parental email or concerned by any aspect, seek advice from your line manager or a senior member of staff.

5.6 Email communication with Pupils

5.6.1 Teachers need to ensure that email contact is professional and should use official school email addresses only. You **must** also copy in the child's tutor to any reply. You **must** adhere to the Safeguarding and Child Protection Policy.

If you are unsure how to respond to a pupil email or concerned by any aspect, seek advice from your line manager or a senior member of staff.

5.7 Tackling problems

5.7.1 Where staff feel that colleagues are not making efforts to abide by the contents of this guidance it is reasonable to:

- Speak with the person who sent the email - ideally in person or by phone - reminding them about the principles within this guidance and encouraging them to follow its advice. All staff should aim to support and remind each other of the importance of respecting boundaries and working in a professional and efficient manner. However, entering into email discussion about appropriateness of emails is discouraged.
- Speak to your line manager in the first instances for a second opinion on email content and further advice if necessary, if you feel it to be inappropriate.
- Try applying a degree of professional empathy to the message sent and consider whether you could be 'reading too much into it'. Feedback to the sender may still be necessary but taking a step back and considering whether the issue is typical in your experience of an individual may separate a 'one-off' from a more serious issue.

5.8 'Rule of Thumb' email guidance

In terms of what is currently considered good practice:

Consider whether an email is the most effective method of communicating your message. It may be more productive to have a quick face to face meeting or phone call followed up with one summary email to confirm discussions (if necessary).

Remain respectful, treating others with dignity at all times.

Write all email messages in a professional manner. Whilst the written style may sometimes differ, the general content of a work email should be consistent to other forms of written communication.

Keep emails short and to the point wherever possible.

Re-read emails before sending from the perspective of the recipient(s).

Do not leave the subject line blank.

Ensure appropriate use of cc. and whether all participants of an email need to continue to be cc. ed or included in an email trail when the topic deviates to another issue.

Be extremely cautious in the use of bcc. ensuring that decisions to do so would meet the standards of integrity and transparency.

Try to minimise the use of graphics, different fonts, and formats stored within a document when sending it as an attachment to an email.

Be extremely careful when sending emails containing personal or confidential information.

Check the recipient's name, especially if there is more than one person with the same name.

Before commencing writing an email on a sensitive topic, consider talking confidentially in person or by phone instead. If there is a possibility that the email will be misconstrued, misunderstood or intercepted, it is probably best avoided.

Do not expect others to wade through extensively long email trails to pick up important information you wish them to be aware of.

Avoid using uppercase text unless completely appropriate and necessary for particular emphasis (e.g. acronyms or initials of names), as this is often interpreted as electronic "shouting".

Be careful when using humour or sarcasm within an email as this can be easily misinterpreted.

It is accepted that emails may be prepared and sent outside of normal school timetable hours, however, replies should not be expected before the next working day commences.

Automated 'out of office' notifications can be used to manage expectations for both the recipient and sender of emails (e.g. by explaining the time of return to work following a period of time off work, period of back-to-back meetings, exam times etc.). Where possible it is helpful to ensure an appropriate signposted alternative is suggested.

Apart from emails to the office regarding attendance for example, emails should not be written or sent during registration or lessons. It is also inappropriate to look at emails during meetings.

6. Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- DfE (2022) 'Keeping children safe in education 2022'
- DfE (2023) 'Generative artificial intelligence in education'
- DfE (2023) 'Meeting digital and technology standards in schools and colleges'
- JCQ (2023) 'Artificial Intelligence (AI) Use in Assessments: Protecting the Integrity of Qualifications'
- JCQ (2023) 'Suspected Malpractice Policies and Procedures'

This policy operates in conjunction with the following school policies:

- Social Media and Online Safety Policy
- Data Protection Policy (within Information, Records and Copyright: Policy and Procedures)
- Safeguarding and Child Protection Policy
- Examination: Remarking & Resitting Policy

7. Roles and responsibilities

The governing board will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Reviewing this policy on an **annual** basis.
- Ensuring their own knowledge of the use of AI tools in the school is up-to-date.
- Ensuring all staff undergo child protection and safeguarding training, including online safety, at induction and at regular intervals.
- Ensuring the school follows the DfE's digital and technology standards.

The headteacher will be responsible for:

- Ensuring that staff receive regular, up-to-date training on how to use AI tools in school.
- Ensuring that the use of AI tools in the school is integrated into relevant policies and procedures, the curriculum and staff training.
- Communicating with parents to ensure they are kept up-to-date with how AI tools are being used in the school, how this will impact pupils' education and how the school is ensuring the tools are being used safely and effectively.
- Working with the governing board to review and update this policy on an **annual** basis.
- Ensuring that AI practices are audited and evaluated on a regular basis.

ICT technicians will be responsible for:

- Providing technical support in the development and implementation of the school's AI practices, policies and procedures.
- Implementing appropriate security measures.
- Ensuring that the use of AI tools is taken into consideration when creating policies and procedures regarding online safety, child protection and safeguarding, and data protection.

The DPO will be responsible for:

- Keeping up-to-date and informed with AI technologies relevant to the school.
- Understanding and maintaining awareness of what the use of AI means for data protection in the school.
- Advising the school on how to integrate the use of AI while complying with data protection regulations.

The DSL will be responsible for:

- Taking the lead responsibility for online safety in school.
- Undertaking training so they understand the risks associated with using AI tools in school.
- Liaising with relevant members of staff on online safety matters.
- Maintaining records of reported online safety concerns relating to the use of AI tools, as well as the actions taken in response to concerns.
- Reporting to the governing board about the use of AI tools and how it links to safeguarding on a **regular** basis.

All staff members will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Taking responsibility for the security of the AI tools and data they use or have access to.
- Modelling good online behaviours when using AI tools.
- Maintaining a professional level of conduct in their use of AI tools.
- Having an awareness of the risks that using AI tools in school poses.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring that the safe and effective use of AI tools is embedded in their teaching of the curriculum.

- Familiarising themselves with any AI tools used by the school and the risks they pose.

Pupils will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from the relevant school staff if they are concerned about an experience that they or a peer has experienced while using AI tools.
- Reporting concerns in line with the school's reporting procedure.
- Familiarising themselves with any AI tools used by the school and the risks they pose.

8. Data protection and cyber-security

The school is aware of the data privacy and cyber-security implications that come with using generative AI tools, and will ensure that all AI tools are used in line with the school's Data Protection Policy and Cyber-security Policy. The school will follow the procedures in these policies to continue to protect pupils from harmful online content that could be produced by AI tools.

The school will not enter data that is classed as personal and sensitive into AI tools under any circumstances. Any data entered will not be identifiable, and will be considered released to the internet.

All staff will be made aware that generative AI tools are able to create believable content of all kinds, for example credible email scams requesting payment, and that the content AI produces may seem more authoritative and believable than usual scams. All staff will apply their best judgement and common sense to manage cyber-security risks effectively and ensure that the DfE's cyber standards are followed at all times.

9. Monitoring and review

The governing board and headteacher will review this policy in full on an **annual** basis, and following any incidents that occur due to the use of AI tools, e.g. data protection or cyber-security.

The next scheduled review date for this policy is **date**.

Any changes made to this policy are communicated to all members of the school community.

Appendix 1: Student acceptable use agreement (students and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my username and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I'm finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement (staff, Trustees, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, TRUSTEES, VOLUNTEERS AND VISITORS	
Name of staff member/Trustee/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/Trustee/volunteer/visitor):	**Date:**