Thurnby Mead Primary Academy

TMET IT Online Safety Policy

This policy is effective for all schools within The Mead Educational Trust, the Teaching School, the SCITT and all other activities under the control of the Trust and reporting to the Trust Board.

This policy should be read in conjunction with the Acceptable User Policy (AUP), Online Infringements and Sanctions (see Appendix 1), Safeguarding and Child Protection Policy, Anti-Bullying Policy, PSHE and Computing Policy,

Version:	10.0
Ratified by:	Executive Team
Date ratified:	6th October 2026
Review date:	September 2027 (annual review)

Revision History:

Version	Date	Author	Summary of Changes:
Earlier version history is available on request.			
10.0	Sept 2026	GSM & MPA	General formatting and tidy, including job title changes. Updated to reflect KCSIE 2026. Section 4.8 Password Policy updated to confirm when requirement of immediate password reset is required. Section 4.13 Emailing Personal, Sensitive…Information updated, specifying Microsoft access-controlled and cloud links and encryption for information sharing. Section 4.19 updated ICO link Section 9: Social Media updated to reflect TMET photography and videography standards. Appendix 1: Online Safety Infringements and Sanctions tables updated.

TMET IT Online Safety Policy

Contents

1. Introduction and Overview 2
2. Education and Curriculum 9
3. Expected Conduct and Incident Management 10
4. Managing IT and Communication Systems 12
5. Data Security - Management Information System access and data transfer 24
6. Equipment and Digital Content 24
7. Home Learning 26
8. Communications 30
9. Social Media - Protecting Professional Identity 31
10. Online Safety Infringements & Sanctions 31
11. Appendix 1 - Online Safety Infringements and Sanctions 38

1. Introduction and Overview

1.1. Purpose

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with other school policies].
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

TMET recognises that online risks continue to evolve and that safeguarding arrangements must respond to emerging technologies and behaviours.

Content

Exposure to harmful, inappropriate or illegal content, including:

- Racist, discriminatory or hate-based content.
- Misogynistic or gender-based abuse.
- Self-harm and suicide content.
- Pornographic content.
- Radicalisation and extremism.
- Misinformation, disinformation and conspiracy theories.

- Harmful social media trends.
- AI-generated harmful content.
- Deepfake images, videos and audio.
- AI-generated intimate images and nudification content.
- Content promoting harmful behaviours, violence or exploitation.

Contact

Being subjected to harmful online interaction with others, including:

- Grooming for sexual, criminal or financial exploitation.
- Adults posing as children or young people.
- Coercion, intimidation or manipulation.
- Harmful interactions through social media, gaming and messaging platforms.
- Exploitation through online communities.
- Harmful interactions with AI chatbots and virtual companions.
- Sextortion and blackmail.
- Online fraud and financial exploitation.

Conduct

Online behaviour that increases the likelihood of harm, including:

- Online bullying and cyberbullying.
- Sexual harassment and abuse.
- Sharing nude or semi-nude images.
- Creating, sharing or possessing AI-generated intimate images.
- Deepfake creation and distribution.
- Impersonation of others online.
- Image-based abuse.
- Abuse through anonymous accounts.
- Harmful online challenges and trends.
- Misuse of artificial intelligence technologies.
- Bypassing filtering and monitoring systems.

Commerce

Risks associated with online financial activity, including:

- Online gambling.
- Financial scams.
- Phishing attacks.
- Identity theft.
- Fraudulent purchases.
- Cryptocurrency and investment scams.
- In-app purchasing exploitation.
- Subscription and payment fraud.

Emerging Technologies

The school recognises that emerging technologies, including generative artificial intelligence, present both opportunities and safeguarding risks.

The school will regularly review emerging risks to ensure pupils are protected from:

- AI-generated harmful content.
- Deepfakes and manipulated media.
- AI-facilitated bullying and harassment.
- AI-assisted grooming or exploitation.
- Data privacy and security risks associated with AI platforms.
- AI-generated misinformation and disinformation.

1.2. Scope

This policy applies to all members of each school within The Mead Educational Trust, Teaching School, SCITT or Trust central offices (including staff, apprentices, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of Trust/School IT systems, both in and out of The Mead Educational Trust. It also applies to use of personal digital technology on the school site (where allowed)

1.3. Roles and Responsibilities

Role	Key Responsibilities
Trust Executive Team	• The TMET Executive Team is responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. • The executive team will receive information about significant online safety incidents along with monitoring reports; which include regular monitoring of online safety incident and filtering / change control logs
Principal	• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Keeping Children Safe in Education (KCSIE) guidance; • To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. • To take overall responsibility for online safety provision; • To be responsible for ensuring that all staff including the Designated Safeguarding Lead (DSL), IT provider and technical staff carry out their role effectively and they are provided with suitable training to enable them to carry out their safeguarding and online safety roles; • To be aware of procedures to be followed in the event of a serious online safety incident; • Ensure suitable 'risk assessments' undertaken so the curriculum meets the needs of students, including risk of children being radicalised; • To ensure they receive regular monitoring reports for the DSL. • To ensure annual filtering and monitoring reviews are completed and recorded. • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures; • To ensure Academy Councillors are regularly updated on the nature and effectiveness of the school's arrangements for online safety; • To ensure school website includes relevant information.

	• Ensure they work with the DSL and IT service provider in all aspects of filtering and monitoring and cyber security
Designated Safeguarding Lead	• Take day to day responsibility for online safety within their safeguarding role. • Lead the strategic oversight of filtering and monitoring arrangements. • Ensure filtering and monitoring arrangements meet the needs of the school community. • Ensure filtering and monitoring arrangements meet the needs of the school community. • Lead the annual review of filtering and monitoring systems. • Ensure records of reviews, testing and actions are maintained. • Monitor emerging online risks, including those linked to generative artificial intelligence (AI). • Report findings, risks and actions to the Academy Council and Trust Board through safeguarding reporting arrangements. • Ensure filtering and monitoring remains proportionate to the age, needs and vulnerabilities of pupils. • Ensure AI-related safeguarding incidents are managed in accordance with safeguarding procedures. • Receive regular and relevant online safety training to help them understand the risks and feel confident in keeping children safe online. • Promote an awareness and commitment to online safety throughout the school community; • Ensure that online safety education is embedded within the curriculum; • Liaise with the Trust IT team where appropriate; • To communicate regularly with SLT and the Academy Council to discuss current issues, review incident logs and filtering/change control logs; • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident; • To ensure that online safety incidents are logged as safeguarding incidents and actioned appropriately; • Facilitate training and advice for all staff; • Oversee any student surveys / feedback on online safety issues; • Liaise with the Local Authority and relevant agencies; • Is regularly updated in online safety issues and legislation and be aware of the potential for serious child protection concerns.
TMET Safeguarding Trustee and Director of Education with responsibility	• To ensure that the school has in place policies and practices to keep the children and staff safe online; • Review the implementation of the Trust Online Safety Policy and review the effectiveness of the policy; • To support the school in encouraging parents and the wider community to become engaged in online safety activities;

for Safeguarding	• Work alongside school DSLs to monitor online safety incidents and student alerts produced by the monitoring software. . • Work alongside the school DSLs and IT team to review blocked websites. • Receive assurance that the Trust's filtering and monitoring systems are reviewed annually and meet the Department for Education's filtering and monitoring standards. • Receive annual review outcomes • Scrutinise online safety data • Provide challenge regarding AI and cyber security risks.
School Computing Curriculum Leader	• Work with the DSL to develop a planned and coordinated online safety curriculum • Liaise with the DSL to ensure the online safety curriculum is planned, mapped, embedded and evaluated for effectiveness including pupil voice.
Trust Head of IT Services	• To report online safety related issues that come to their attention, to the Designated Safeguarding Lead; • To manage the Trust/School network and make sure that the Trust/School technical infrastructure is secure and is not open to misuse or malicious attack; • the school meets required online safety technical requirements; • school password policy is strictly adhered to and reset termly for all users; • access controls/encryption exist to protect personal and sensitive information held on school-owned devices; and • the Trust's policy on web filtering is applied/updated on a regular basis and that its implementation is not the sole responsibility of any single person. • Ensure the use of school technology, online platforms and email are regularly monitored and that any misuse/attempted misuse is reported to the Principal; • To ensure appropriate backup procedures and disaster recovery plans are in place; • To keep up-to-date documentation of the school disaster recovery plans • To ensure the school uses appropriate IT systems and services including, filtered Internet Service • To ensure that the IT Team is up to date with online safety technical information in order to effectively carry out the school's online safety responsibilities • To ensure that monitoring systems are implemented and updated as agreed in the Trust/School policies • To ensure that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
Data Managers /	• To ensure that the data they manage is accurate and up to date

Administrators	• To ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements
Teachers	• To have awareness of current online safety matters/trends and of the current online safety policy and practices. • To understand that online safety is a core part of safeguarding. • To teach online safety effectively within the curriculum; • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant); • To ensure that pupils are fully aware of research skills and the need to avoid plagiarism and are fully aware of copyright regulations in relation to electronic content. • To ensure there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc. • To model safe, responsible and professional online behaviours in their own use of technology, including out of school and in their use of social media. • To adhere to the school's Online Safety and Acceptable Use Policies, with regard to the use of devices, systems and passwords and have an understanding of basic cyber security. • To understand how pupils use digital technologies out of school, so they can recognise online safety issues that may arise. • To understand the benefits and risk of Artificial Intelligence (AI) in school and be open about how it is used
All staff, volunteers and contractors.	• To read, understand, sign and adhere to the Staff Acceptable Use Agreement/Policy, and understand any updates annually. The AUP is signed by new staff on induction; • To report any suspected misuse or problem to the Principal; • To maintain an awareness of current online safety issues and guidance e.g. through CPD; • To model safe, responsible and professional behaviours in their own use of technology. • All digital communications with pupils / parents / carers should be on a professional level and only carried out using official Trust/School systems • Monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Policy annually, by accepting the AUP upon sign in; • To understand the importance of reporting abuse, misuse or access to inappropriate materials;

	• To know what action to take if they or someone they know feels worried or vulnerable when using online technology; • To understand and take care when using AI services and check the accuracy of content accessed through AI • To understand the risks associated with AI, including deepfakes and deep nudes • To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of the school
Parents/carers	• Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, letters and the school website. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of: • digital and video images taken at school events (as per Parent and Visitor Code of Conduct) • access to parents' sections of the website and online pupil records • their children's personal devices in the school (where this is allowed) • Other responsibilities include; • To read, understand and promote the school's Pupil Acceptable Use Agreement with their child/children; • To consult with the school if they have any concerns about their children's use of technology; • To support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images.
External groups including Parent groups	• Any external individual/organisation will sign an Acceptable Use Agreement prior to using technology or the Internet within the school; • To support the school in promoting online safety; • To model safe, responsible and positive behaviours in their own use of technology.

1.4. Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be shared with the staff and whole school community via the school website
- Policy to be part of school induction pack for new staff, through Safeguarding training including online safety which includes an understanding of their role in relation to online safety.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and pupils at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to the school.

1.5. Handling Incidents:

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- Designated Safeguarding Lead acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to the Principal and Trust IT team that day.
- Any concern about staff misuse is always referred directly to the Principal, unless the concern is about the Principal in which case the complaint is referred to the Trust Chief Executive Officer.
- Where AI is used to support monitoring, human oversight is maintained to interpret nuances and context that AI might miss.

(See Appendix 3 & Section 9 - Online Safety Infringements and Sanctions)

2. Education and Curriculum

2.1 Pupil Online Safety Curriculum

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, including the following areas:

- A planned online safety education programme covering a range of skills and behaviours appropriate to their age and experience, including
    - How to identify deepfake content
    - How AI can manupilate images, audio and video
    - How algorithms influence onlien content
    - Risk assosicarefd with harmful influencers
    - Risk associated with Misogny
    - Violence againt girls and women
    - Financial scams and online fraud
    - Safe use of AI tools.
- Lessons are context relevant with agreed objectives leading to clear and evidenced outcomes.
- A focus on building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making;
- Pupils should be taught in all lessons to think carefully about information they find online and check if its accurate, including content from Artificial Intelligence.
- Responsibilities of pupils, according to the Pupil Acceptable Use Agreement(s); Issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- Ensuring pupils know to only use school approved systems and publish within appropriately secure / age-appropriate environments;
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the website's students visit;

- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT support team can temporarily remove those sites from the filtered list for the period of study. Any request to do so, will be auditable, with clear reasons.

2.2 Staff, Academy Councillor and Volunteer training

This school:

- Makes regular training available to staff, Academy Councillors and volunteers, on online safety issues, generative AI risk, deepfakes, cyber security awareness and the school online safety education program; this will be an integral part of the school's annual safeguarding training.
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy, filtering and monitoring responsibilities and the school's Acceptable Use Agreements.
- Provides advice / guidance / training to individuals as required
- Will share this Online Safety policy and updates with staff during training days and/or briefings
- Ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright
- Ensures that staff understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- Ensures that staff understand that they can request temporary access to websites that are normally filtered. This must be for educational purposes and clearly part of the curriculum, e.g. drugs, discrimination, historical weaponry. Requests are logged and saved by the Trust IT team.

2.3 Parent awareness

The school will seek to provide information and awareness to parents and carers through:

- Letters, communication systems, website
- Parents' evenings
- Events / campaigns e.g. Safer Internet Day
- Reference to the relevant websites and publications

3. Expected Conduct and Incident Management

3.1 Expected conduct

In this school all users:

- Are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- Understand the significance of misuse or access to inappropriate materials and are aware of the consequences;

- Understand it is essential to report abuse, misuse or access to inappropriate materials and know how to do so;
- Understand the importance of adopting good online safety practice when using digital technologies in and out of the school;
- Know and understand school policies on the use of mobile and handheld devices including cameras.

3.2 Staff, volunteers and contractors

- Know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older students have more flexible access;
- Know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (student friendly) search engines where more open Internet searching is required with younger pupils.

3.3 Parents/Carers

- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form;
- Should know and understand what the school's rules of appropriate use for the whole school community are and what sanctions result from misuse.

3.4 Incident Management

In this school:

- There is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;
- Online safety incidents involving AI-generated content, deepfakes, nudification applications, image-based abuse or digitally manipulated content will be recorded and managed as safeguarding concerns where appropriate."
- All members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's safeguarding and child protection policy, child-on-child abuse procedures and behaviour policy;
- Support is actively sought from other agencies as needed (e.g. UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, Internet Watch Foundation) in dealing with online safety issues;
- All online safety incidents are monitored and recorded on CPOMs/Bromcom/Arbor/SIMS and analysed for themes, trends and emerging risks. This also contributes to developments in policy and practice in online safety within the school;
- Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- The Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- We will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation etc.

(See Section 9 & Appendix 3 - Online Safety Infringements and Sanctions)

3.5 AI-Generated Child-on-Child Abuse

TMET recognises that advances in artificial intelligence (AI) have created new risks which may facilitate child-on-child abuse.
AI-generated content may be used to cause harm, humiliate, exploit, threaten or sexually harass others and will be treated as a safeguarding concern.
Examples may include:

- AI-generated intimate images.
- Deepfake images, audio or video.
- Nudification applications.
- Digitally manipulated sexualised images.
- Image-based sexual abuse.
- Impersonation of pupils or staff.
- Harassment, bullying or discrimination using AI-generated content.
- Distribution of manipulated images without consent.
- Coercion, blackmail or sextortion using AI-generated material.

The school recognises that AI-generated content can have the same impact on victims as other forms of child-on-child abuse and will respond to incidents in accordance with the Child Protection and Safeguarding Policy, Behaviour Policy and Online Safety Policy.
All reports will be taken seriously and managed on a case-by-case basis.
The school will:

- Provide support to any child affected.
- Assess and manage risk.
- Secure and preserve evidence where appropriate.
- Consider whether the behaviour constitutes child-on-child abuse, sexual harassment, sexual violence or another safeguarding concern.
- Involve parents/carers where appropriate.
- Work with external agencies where required.
- Consider disciplinary action where appropriate.
- Make referrals to Children's Social Care, Police or other agencies where the threshold for intervention is met.

Where incidents indicate that a child may be suffering, or is likely to suffer, significant harm, the Designated Safeguarding Lead will follow local safeguarding procedures and relevant referral pathways.
The creation, possession, sharing or distribution of AI-generated intimate images of children may constitute a criminal offence and will be managed in line with statutory safeguarding guidance and advice from the Police.

4. Managing IT and Communication Systems

4.1 Internet access, security (including virus protection) and filtering

This school:

- Informs all users that Internet/email use is monitored;

- Has filtered secure broadband connectivity through connectivity providers and effective web/content filtering solutions;
- Ensures the school internet access includes filtering appropriate to the age and maturity of pupils either directly through internet provider or 3rd party solutions;
- Provides enhanced / differentiated user-level filtering through on-site and cloud-based filtering systems;
- Works with the internet connectivity and 3rd party filtering solution providers to ensure that filtering procedures are continually reviewed;
- Has a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure through acceptable use policies and training;
- Ensure that, if staff or pupils discover safeguarding concerns on websites, the URL will be reported to the Principal who will then record the incident and escalate the concern as appropriate;
- Has a filtering system which will block all sites on the Internet Watch Foundation (IWF) and Counter-Terrorism Internet Referral Unit (CTIRU) lists;
- Ensures that changes to the school filtering procedures will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team;
- Has effective filtering and moderation of Generative AI products, platforms and features, to reliably prevent access to harmful and inappropriate content by users;
- The school Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective;
- Ensures that any material that the school believes is illegal will be reported to appropriate agencies such as IWF, the Police or CEOP;
- Has an access strategy designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers;
- Ensures that changes to the filtering policies are updated by the Trust Head of IT Services as directed by the school Senior Leadership Team;
- Ensures that appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school/Trust systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date active virus/malware software.
- Forbids all users from downloading executable files and installing programs on school owned devices without approval from IT Support and/or the Senior Leadership Team.
- Prohibits any attempt to bypass, disable, or circumvent school filtering and security controls. Including, but not limited to, the use of unauthorised VPNs, proxy websites or tethering of school devices to personal mobile hotspots;
- Prohibits all users from authorising third-party applications, browser extensions, or cloud integrations using their school Google/Microsoft credentials (Single Sign-On) without explicit approval from the Trust IT Team;
- Ensures network health through use of suitable anti-virus software;
- Uses DfE approved systems including DfE S2S, to send 'protect-level' sensitive / personal data over the Internet;
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site.

- Ensures that servers, wireless systems and cabling are securely located and physical access restricted.

4.2 Filtering and Monitoring Standards

The school will ensure that filtering systems:

- Are configured to reliably block and mitigate access to illegal, inappropriate and harmful content.
- Are applied to all users, devices and internet connections used within the school.
- Are appropriate to the age, needs and vulnerability of pupils.
- Are regularly reviewed and updated in response to safeguarding concerns, incidents and emerging risks.
- Take account of developments in technology, including artificial intelligence and generative AI tools.

The school will ensure that monitoring systems:

- Identify potential safeguarding concerns, wellbeing concerns and online safety risks.
- Detect indicators of misuse, cyber security threats and attempts to bypass safeguarding controls.
- Alert appropriate staff to concerns in a timely manner.
- Provide reporting information that supports effective safeguarding oversight, review and decision-making.

Filtering and monitoring arrangements will be reviewed regularly to ensure they remain effective, proportionate and compliant with the Department for Education's filtering and monitoring standards.

4.3 Annual Review of Filtering and Monitoring

The school recognises that filtering and monitoring is a safeguarding responsibility and forms part of the school's wider safeguarding arrangements.

The effectiveness of filtering and monitoring systems will be formally reviewed at least once during every academic year.

The review will:

- Be led by the school's Filtering and Monitoring Lead.
- Include the Designated Safeguarding Lead and Trust IT Team.
- Assess compliance with the Department for Education Filtering and Monitoring Standards.
- Test filtering and monitoring arrangements across all internet-connected devices.
- Consider risks associated with generative AI, social media, messaging platforms and emerging technologies.
- Consider the age, developmental needs and vulnerabilities of pupils.
- Review incidents, alerts, safeguarding concerns and trends.
- Identify actions required to strengthen safeguarding arrangements.
- Be documented and retained for governance and assurance purposes.

The outcome of the review will be reported to the Academy Council and appropriate Trust safeguarding forums.

4.4 Generative AI, Filtering & Monitoring

"Generative AI" means a system or product that can generate content in response to user inputs, including, text, images, video or audio and which may adapt or be fine-tuned. The section applies to any generative AI – whether supplied by the school, by third-party providers or access by students or staff via external tools.

This school:

- Ensures that technical safeguards are in place to reduce the risk of users generating or accessing harmful and inappropriate content when using generative AI systems, tools or platforms;
- Maintains filtering standards that are effective throughout the duration of a conversation or interaction with a user;
- Adjusts filtering based on different levels of risk, age, appropriateness and the user's needs – for example users with special educational needs and disabilities (SEND);
- Ensures multimodal content is effectively moderated, including detecting and filtering prohibited content across multiple languages, images, common misspellings and abbreviations. Ensure full content moderation capabilities are enforced regardless of the device used, including bring your own device (BYOD) and smartphones when accessing products via a school/Trust account;
- Moderates content based on an appropriate contextual understanding of the conversation, ensuring that generated content is sensitive to the context;
- Updates filtering in response to new or emerging types of harmful content.
- Ensure that any generative AI platform, tool or system is subject to an appropriate assessment prior to use, including consideration of safeguarding risks, privacy and data protection risks, cyber security risks, age appropriateness and effectiveness of content moderation controls;
- Ensure prohibited use of AI, including the creation, possession, sharing or distribution of AI-enabled impersonation or AI-enabled blackmail, are prevented wherever reasonably possible and managed as safeguarding concerns where identified.

In addition, this school also:

- Ensures that all generative AI products used are audited prior to use based on the brief outlined in this section of the Online Safety Policy;
- Provides only access to generative AI products that maintain robust activity logging procedures by recording input prompts and responses, analysing performance metrics and alerting DSLs when harmful and inappropriate content is access or attempted to be accessed;
- Alerts and signposts the user to appropriate guidance and support resources when access of prohibited content is attempted;
- Identifies and alerts DSLs of potential safeguarding disclosures made by users;
- Generates reports and trends on access and attempted access of prohibited content, in a format that non-expert staff can understand.

All Generative AI platforms, tools or systems used by users will comply with the following security, privacy and Governance expectations:

- Offer robust protection against 'jailbreaking' by users trying to access prohibited material;

- Offer robust measures to prevent unauthorized modifications to the product that could reprogram the products functionality;
- Allow administrators to set different permission levels for different users;
- Ensure regular bug fixes and updates are promptly implemented;
- Sufficiently test new versions or models of the product to ensure safety compliance before release;
- Have robust password protection or authentication methods;
- Be compliant with the Cyber Security Standards for Schools and Colleges;
- Complete a DPIA (Data Protection Impact Assessment) prior to use by school/Trust users;
- Undertake risk assessments prior to use by school.

4.5 Use of Artificial Intelligence (Generative AI)

The school recognises that generative AI tools can support teaching, learning, and professional practice when used safely and responsibly. All staff, pupils, and parents/carers must adhere to the Acceptable Use Policy, which includes guidance on the use of AI.

4.6 AI-Generated Harm and Safeguarding

The school recognises that generative AI creates safeguarding risks that may affect pupils, staff and the wider school community.
Examples include:

- AI-generated intimate images.
- Nudification applications.
- Deepfake images, audio and video.
- Identity impersonation.
- Harassment and bullying.
- Sextortion.
- Grooming.
- Manipulation and coercion.
- AI-generated misinformation and disinformation.

Any incident involving AI-generated harm will be treated as a safeguarding concern and managed in accordance with the Child Protection and Safeguarding Policy.

Where appropriate, incidents may also be managed under:

- Child-on-child abuse procedures.
- Behaviour procedures.
- Anti-bullying procedures.
- Staff disciplinary procedures.
- Criminal investigation processes.

Permitted use of AI

AI tools may be used for educational and professional purposes, including:

- Research and information gathering.
- Idea generation to support projects, planning or lesson preparation.

- Analysing text in order to identify improvements or recommendations.
- Producing summaries or explanations of topics and concepts for revision, lesson support, or professional development.

Unauthorised use of AI

AI tools must not be used in ways that risk harm to individuals, compromise safeguarding, prevent duties or breach the school's policies. Prohibited use includes (but is not limited to):

- Generating or attempting to generate inappropriate, offensive or harmful content, including images .
- Uploading or entering personal details of staff, pupils, parents, or other individuals into AI systems.
- Using AI to humiliate, bully, intimidate, or cause harm to others.
- Using AI tools to bypass safeguarding measures, filtering, or assessment integrity.

Examples of misuse

The following activities are also considered infringements of this policy:

- Deepfakes and gendered images
- Copying or paraphrasing AI-generated content so that submitted work does not reflect the user's own understanding, analysis, evaluation, or calculations.
- Submitting AI-generated work without appropriate acknowledgement of the tool used.
- Providing incomplete or misleading references to AI sources.
- Uploading copyrighted, proprietary, or sensitive content into AI systems without permission.
- Using AI outputs in a way that brings the school, Trust, or its community into disrepute.

Labelling and acknowledgement

Where AI tools have been used to support teaching, learning, or professional tasks, staff and pupils must clearly label and acknowledge their use.

Privacy and copyright

Neither staff nor pupils' personal information (e.g. names, photographs, contact details) must be uploaded to AI tools. All users are expected to respect intellectual property rights and ensure that AI-generated text, images, or other content does not infringe copyright.

4.7 Network management (user access, backup)

This school:

- Uses individual, audited logins for all users (KS2 and above);
- Uses guest accounts occasionally for external or short-term visitors for temporary access to appropriate services;
- Uses teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful;
- Has local network monitoring/auditing software installed;
- Has daily back-up of school data (admin and curriculum);
- Uses secure, 'Cloud' storage for data back-up that conforms to DfE guidance;
- Uses storage of all data within the school which conforms to the EU and UK data protection requirements; Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password;
- Gives pupils their own unique username and password (KS2 and above) which gives them access to the Internet and other services;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to log off when they have finished working or are leaving the computer unattended;
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities;
- Maintains equipment to ensure Health and Safety is followed;
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data;
- Uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system;
- Has a wireless network that has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- Ensures that all IT and communications systems are installed professionally and regularly reviewed to ensure they meet health and safety standards.

The Trust recognises that cyber security is a safeguarding issue. Cyber incidents may:

- Disrupt safeguarding systems
- Expose sensitive pupil information
- Increase vulnerability to exploitation
- Compromise safeguarding records

The Trust and all member schools are committed to meeting and maintaining the DfE Cyber Security Standards. The Trust, and therefore the school;

- Will carry out annual cyber risk assessments and review termly.
- Has identified the most important and critical part of its digital system and made sure they are protected against cyber security threats.
- Has strong backup and recovery plans, and ensures critical digital systems are secure.
- Ensures that staff and governors receive training on common cyber threats, and learners are taught cyber awareness.
- Has clear business continuity and incident management in place.

- Policies reflect the importance of cyber security, and there are clear procedures for reporting incidents. Everyone is expected to report any cyber risks or concerns and should feel safe doing so.

4.8 Password policy

All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.

This school:

- Makes it clear that staff and pupils must always keep their passwords private and must not share with others. If a password is compromised the school should be notified immediately;
- Requires staff to use STRONG passwords;
- Requires staff to change their passwords into the Trust System and MIS (i.e. Bromcom) twice a year.
- Requires all staff using trust/school systems to use multi factor authentication for all systems that support MFA, prioritising safeguarding, MIS, cloud storage and email systems;;
- Monitors cloud based systems for potentially dangerous logins, mitigating the risk through Multifactor authentication challenges, physical location restrictions and lockout policies.
- Requires passwords to be reset immediately if compromise is suspected or detected.

4.9 Responsibilities:

All users (adults and pupils KS2 and above) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. KS1 pupils will make use of a single “class login” which will be monitored by the staff members responsible for the pupils at that point in time.

The management of password security will be the responsibility of the Trust Systems Manager. Passwords for new users, and replacement passwords for existing users can be allocated by the IT Support team. Any changes carried out must be notified to the member of staff responsible for issuing and coordinating password security (above).

4.10 Training/Awareness:

It is essential that users are made aware of the need to keep passwords secure, and the risks attached to unauthorised access/data loss. This should apply to even the youngest of users, even if class logons are being used.

Members of staff will be made aware of the school’s password security procedures:

- at induction;
- through the school’s Online Safety Policy and procedures;
- through the Acceptable Use Agreement;

Pupils will be made aware of the school’s password security procedures:

- in ICT and/or Online Safety lessons
- through the Acceptable Use Agreement

The following rules apply to the use of passwords:

- the last four passwords cannot be re-used;
- the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special character;
- the account should be "locked out" following six successive incorrect log-on attempts;
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on;
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption);
- requests for password changes should be authenticated to ensure that the new password can only be passed to the genuine user.

The "master/administrator" passwords for the school ICT systems, used by the Trust Head of IT Services and IT Systems Manager must also be available to the Senior Leadership and kept in a secure place, referenced via the School/Trust BCP. The school should never allow one user to have sole administrator access.

4.11 Audit/Monitoring/Reporting/Review:

The Trust Head of IT Services will ensure that full records are kept of:

- User IDs and requests for password changes;
- User logons;
- Security incidents related to this Policy and procedures.

In the event of a serious security incident, the Police may request and will be allowed access to passwords used for encryption. Local Authority Auditors also have the right of access to passwords for audit investigation purposes.

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner. These records will be reviewed by the central Trust team at regular intervals.

4.12 E-mail

The Trust:

- Provides staff with an email account for their professional use, and personal email should be through a separate account;
- Uses anonymous or group e-mail addresses, for example info@tmet.uk;
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law;
- Will ensure that email accounts are maintained and up to date;
- Will use a number of technologies to help protect users and systems in the school;
- Expects staff to only use official school provided email accounts to communicate with pupils and parents, as approved by the Senior Leadership Team;
- Does not permit the forwarding of chain messages;

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access);
- Users need to be aware that email communications may be monitored.

4.13 Emailing Personal, Sensitive, Confidential or Classified Information

- Assess whether the information can be transmitted via access-controlled OneDrive or SharePoint links (restricted to specific recipients) rather than sending attachments;
- The use of any other Internet based personal webmail service for sending emails containing sensitive information is not permitted;
- Where your conclusion is that email must be used to transmit such data:
    - Obtain express consent from your manager to provide the information by email;
    - Exercise caution when sending the email and always follow these checks before releasing the email:
        - Verify the details, including accurate email address, of any intended recipient of the information;
        - Verify (by phoning) the details of a requestor before responding to email requests for information;
        - Do not copy or forward the email to any more recipients than is absolutely necessary.
    - Do not send the information to any person whose details you have been unable to separately verify (usually by phone);
    -
    - Where cloud link sharing is not supported by the external recipient, send the information as an encrypted document attachment;
    - Provide the encryption key or password by a separate contact with the recipient(s);
    - Do not identify such information in the subject line of any email;
    - Request confirmation of safe receipt.

Pupils:

Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff:

Staff will use the e-mail systems for professional purposes;

Access in school to external personal email accounts may be blocked;

Never use email to transfer staff or student personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

4.14 School website / Teaching School / SCITT

The Principal or Executive Team, takes overall responsibility to ensure that the website content is accurate, and the quality of presentation is maintained;

The school website complies with statutory DFE requirements;

Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;

Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

4.15 Cloud Environments

Uploading of information on the school's online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;

Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community;

In the school, pupils are only able to upload and publish within school approved 'Cloud' systems.

4.16 Home Learning Systems (please refer to Section 7 of this policy: Home Learning)

Home learning platforms are monitored using Trust/School systems and strictly for work use only;

Uploading of information, files and resources to the Trust online learning platform is accessible by staff members according to their responsibilities.

Restrictions and procedures have been introduced to reduce the risk of cyber threats whilst using the Home Learning platform – staff guidance is regularly circulated on best practices;

The Trust and respective Academies reserve the right to disable users access to Remote Learning platforms in the event of misuse, investigation or other appropriate scenarios;

All staff, pupils & other temporary users should read and accept the TMET Acceptable Use for Home Learning policy prior to use of Home Learning platforms (Microsoft Teams).

4.17 Social networking

5.15.1 Staff, Volunteers and Contractors

Staff should refer to the Trust's **Social Media Policy**.

Staff are instructed to always keep professional and private communication separate;

Teachers are instructed not to run social network spaces for pupil use on a personal basis or to open up their own spaces to their pupils, but to use the school's preferred system for such communications.

5.15.2 Pupils

Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work;

Are required to sign and follow our Primary Pupil Acceptable Use Agreement.

5.15.3 Parents

Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required;

Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

4.18 CCTV

Please refer to the Trust's **CCTV Policy**.

We use CCTV in TMET schools where appropriate. This is part of our site surveillance for staff and pupil safety. The use of CCTV is clearly signposted. We will not reveal any recordings without appropriate permission;

We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

4.19 Disposal of Redundant ICT Equipment

All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen.

Disposal of any ICT equipment will conform to:

- The Waste Electrical and Electronic Equipment Regulations 2006
- The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
- Environment Agency Guidance (WEEE) Click here to access
- ICO Guidance – UK GDPR and Data Protection Act 2018 https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/
- Electricity at Work Regulations 1989

The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.

The school's disposal record will include:

- Date item disposed of;
- Authorisation for disposal, including:
- verification of software licensing
- any personal data likely to be held on the storage media*
- How it was disposed of e.g. waste, gift, sale
- Name of person and/or organisation who received the disposed item

* if personal data is likely to be held the storage media will be over written multiple times or 'scrubbed' to ensure the data is irretrievably destroyed.

Any redundant ICT equipment being considered for sale/gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

5. Data Security - Management Information System access and data transfer

5.1 Strategic and operational practices

At this school:

- The Principal is the Senior Information Risk Officer (SIRO);
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners;
- We ensure staff know who to report any incidents where data protection may have been compromised;
- All staff are DBS checked and records are held in a single central record.

5.2 Technical Solutions

Staff have secure area(s) on the network to store sensitive files;

We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes' idle time;

All servers are in lockable locations and managed by DBS-checked staff;

Details of all school-owned hardware will be recorded in a hardware inventory;

Details of all school-owned software will be recorded in a software inventory;

Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website;

Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data;

We are using secure file deletion software.

6. Equipment and Digital Content

6.1 Mobile Devices (mobile phones, tablets and other mobile devices)

Staff are not permitted to use their own mobile devices whilst pupils are present. This includes making or receiving calls or sending texts. Use of personal mobile devices must be restricted to non-contact time, and to areas of the school where students are not present (such as a staff room). There may be circumstances in which it's appropriate for a member of staff to have use of their mobile device during contact time e.g. for emergency contact by their child/their child's school or in the case of acutely ill dependents or family members. In such cases, staff members must seek permission from the principal to allow for special arrangements in advance. If special arrangements are not deemed necessary, staff can use the school office number as a point of emergency contact. Staff must not use their mobile devices to take photographs or recordings of pupils, their work, or anything else which could identify a pupil. If it's necessary to take photos or recordings as part of a lesson/school trip/activity, this must be done using school equipment.
Please refer to TMET's *IT User Policy* for information for supplementary information about usage of mobile devices.

6.2 Pupils' use of personal devices

The school supports the Government expectation that schools maintain a distraction-free and safe learning environment through clear management of pupil mobile phone use.

Thurnby Mead allows children in year 5 and 6 to bring mobile devices to school if they walk home alone. Mobile phones are kept securely at the office and collected by the child at the end of the school day.

If a pupil needs to contact his or her parents or carers, they will be allowed to use the school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office;

If a pupil breaches the school policy, then the device will be confiscated and will be held in a secure place in the school office. Mobile devices will be released to parents or carers in accordance with the school policy.

Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

6.3 Staff use of personal devices

Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting; mobile phone or personally-owned devices must not be used while pupils are present unless express permission has been given by the Principal or school senior leadership team, and only for work-related purposes (e.g. two factor authentication for CPOMs)

Where available, staff will be issued with a school phone where contact with pupils, parents or carers is required, for instance for off-site activities;

Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances or for two factor authentication for CPOMs;

Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose;

In an emergency where a staff member doesn't have access to an school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes;

If a member of staff breaches the school policy then disciplinary action may be taken.

Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.

6.4 Storage, Syncing and Access

The device is accessed with a school owned account

The device has a school created account and all apps and file use are in line with this policy. No personal elements may be added to this device;

PIN access to the device must always be known by the Trust Systems Manager, or possible to reset through Trust management systems;

The device is accessed with a personal account

If personal accounts are used for access to a school owned mobile device, staff must be aware that school use will be synced to their personal cloud, and personal use may become visible in the school and in the classroom;

PIN access to the device must always be known by the network manager;

Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse (if applicable);

6.5 Digital images and video

In this Trust:

- We gain parent/carer permission for use of digital photographs or video involving their child as part of the Media Consent form when their daughter/son joins the school
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term, high profile use;
- Pupils are taught about how images can be manipulated in their online safety education programme, including deepfake identification, AI-generated image risks, image-based abuse and consent and image sharing and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information;
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

7. Home Learning

The Trust recognises that technology can support continuity of education and provide flexible learning opportunities beyond the school environment. Where remote learning is utilised, appropriate safeguards will be implemented to protect pupils, staff and wider school community.

7.1 Teachers

Where remote learning is provided, staff will:

- Use only Trust-approved platforms, applications and communication systems.

- Maintain professional standards and boundaries at all times.
- Teachers will send the invite to pupils for the live lesson the morning of the scheduled lesson. For Secondary schools, pupils will receive an email invitation (calendar) otherwise the lesson can be found within the classroom environment via Microsoft Teams. For Primary schools, pupils will not receive an email and instead pupils will find their lesson links within the Microsoft Teams Classrooms Group.
- Ensure that remote learning activities are appropriate to the age, needs and abilities of pupils.
- Be dressed appropriately and maintain a professional environment when participating in video conferencing or online learning sessions.
- Use neutral and appropriate backgrounds or Trust-approved background features where available.
- Ensure no family members or other individuals are visible, audible or involved in remote learning sessions.
- Communicate with pupils only using authorised Trust communication systems and within agreed working hours. of 8.45am to 3.15pm.
- Ensure that appropriate meeting settings, permissions and participant controls are applied before and during online sessions. Lobby and presenter options will be set and participants checked before admitting to the meeting.
- Monitor pupil engagement and behaviour and address any concerns in accordance with school procedures.
- Report any safeguarding concerns arising from remote learning activities immediately to the Designated Safeguarding Lead (DSL).

Staff must not:

- Conduct one-to-one video sessions with pupils without prior approval from a member of the Senior Leadership Team and consideration of safeguarding arrangements.
- Communicate with pupils using personal social media, messaging services, email accounts or telephone numbers.
- Record, store or share remote learning content in ways that are inconsistent with Trust policies and data protection requirements.

7.2 Use of Artificial Intelligence During Remote Learning

The Trust recognises that Ai may be used to support teaching, learning and administrative activities.

Where AI tools are used during remote learning:

- Only Trust approved and appropriately risk-assessed AI tools may be used.
- Staff must ensure AI-generated content is reviewed for accuracy, appropriateness and suitability before use.
- Personal, safeguarding or confidential information must not be uploaded into AI platforms unless specifically authorised and complaint with Trust data protection requirements.
- Pupils should be taught to critically evaluate AI-generated content and understand its limitations
- Any misuse of AI, including plagiarism, impersonation, deepfake creation or the generation of inappropriate content, will be addressed through safeguarding and behaviour procedures where appropriate.

7.3 Recording of Remote Learning Sessions

The Trust recognises that recording may support safeguarding, accessibility and continuity of learning. All meetings including breakout rooms, with a participant count of 3 or less will be recorded. Recordings of lessons are automatically stored within the chat for 2 weeks and maybe downloaded or shared with the wider class or staff at a later date.
Where recording are used:

- Recording arrangements will be proportionate, transparent and compliant with data protection requirements.
- Participants will be informed where session are being recorded.
- Recording will be stored to the organiser's/teacher's secure OneDrive.
- Access to recording will be restricted to authorised users.
- Retention and deletion of recordings will be managed in accordance with Trust retention schedules and data protection requirements.

7.4 Pupils

Pupils participating in remote learning are expected to:

- Follow the Trust's Acceptable usage policy
- Pupils must be dressed appropriately for the duration of the video lesson, e.g. fully clothed, no pyjamas, no offensive slogans on clothing.
- Teachers will not communicate with pupils outside the hours of 8.50am to 3.00pm (to be customised by the school based on lesson timings); we do not expect you to be working outside of these hours.
- Pupils must remain on mute until invited to talk.
- Pupils should be ready and waiting to learn at the starting time of the lesson – this means your work and writing equipment is out ready and you join the lesson on Microsoft Teams before the start of the lesson.
- Behave in the same respectful manner expected in face-to-face learning.
- Use only their own Trust-issued accounts and login credentials.
- Keep usernames and password secure.
- Participate respectfully and follow staff instructions during online sessions.
- Report any online safety concerns to a trusted adult or member of staff.

<u>Pupils must not</u>

- Record, photograph, screen-record or distribute online lessons without permission.
- Share lesson links, meeting invitations, passwords or access credentials.
- Use AI tools to create harmful, inappropriate, abusive, or deceptive content.
- Disrupt, interfere with or misuse remote learning platforms.
- Use another person's account or allow another person to use their account.

Misuse may result in removal of access, sanctions and safeguarding intervention where appropriate.

7.5 Parents and Carers

Parents and carers play an important role in supporting staff and effective remote learning.

The Trust will encourage parents and carers to:

- Support their child in accessing remote learning safely.
- Ensure children understand expectations for behaviour and online conduct.
- Promote safe use of devices and online learning platforms within the home.
- Monitor their child's use of technology where appropriate.
- Contact the school if they have concerns regarding online safety, behaviour or wellbeing.

Parents and carers should not:

- Record or distribute online learning sessions without authorisation.
- Interrupt or participate in lessons unless specifically invited to do so by the school.
- Share links or access information relating to remote learning sessions.

7.6 Guidance and support for Parents and Carers

- Video-conferencing uses a lot of power, it's a good idea to keep devices plugged into the mains power.
- Do a practice run: role-playing is a great way to prepare your child for what's expected in the video class environment. If you have two devices, you can set yourself up on the platform they'll be using, or just use FaceTime and video-chat as if you're leading the class. Pretend you're the teacher and send your child an invite for a meeting.
- Set expectations for how your child should conduct themselves on camera: face the screen; mute yourself when you're not speaking; unmute yourself when you're ready to talk; turn off the camera if you need to blow your nose; etc.
- Pupils should behave appropriately when learning by video, just the same as if they were in class.
- Assemble necessary equipment: pupils may need earphones, a microphone, and paper and pencil to take notes.
- Choose a neutral background: broadcasting from the bedroom is a little intimate for a class setting. If they must, help them carve out a space where they can have peace and quiet but that doesn't convey too many personal details.
- Don't take devices into the bathroom: just as with regular school, pupils should go to the bathroom before class. If there's an emergency, make sure your child knows how to temporarily disable the video and mute themselves and then turn everything back on again.
- Be respectful of others: as in the class we expect our pupils to be courteous to the teacher and to others. Impress upon them the fact that this is an unusual time for everyone, and appropriate behaviour should be maintained at all times.

7.7 Safeguarding and Monitoring

Remote learning activity undertaken through Trust systems may be subject to monitoring in line with the Trust's safeguarding, filtering and monitoring arrangements.

The school will:

- Monitor online activity through approved filtering and monitoring systems.
- Investigate concerns relating to safeguarding, wellbeing, online safety and misuse of technology.
- Maintain appropriate oversight of interactions that take place through Trust systems.
- Record and respond to safeguarding concerns in accordance with the Safeguarding and Child Protection Policy.

- Review remote learning arrangements regularly to ensure they remain safe, effective and appropriate.

8. Communications

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

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school	x						x	
Use of mobile phones in lessons				x				x
Use of mobile phones in social time	x							x
Taking photos on mobile phones / cameras				x				x
Use of other mobile devices e.g. tablets, gaming devices	x						x	
Use of personal email addresses in school, or on school/Trust network				x				x
Use of school email for personal emails				x				x
Use of messaging apps	x						x	
Use of social media	x						x	
Use of blogs	x						x	

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

- The official school/Trust email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when on the school network, or on school systems (e.g. by remote access).

- Pupils must immediately report to their teacher, and staff to the Principal, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and pupils or parents / carers must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging or social media must not be used for these communications
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff
- Whole class / group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses (in some instances only network accounts – no email account) for educational use.

9. Social Media - Protecting Professional Identity

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues; phishing
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk
- Pupils should not be identifiable in any online content, including social media posts, website articles, blogs, online prospectuses and online films. Photographs and videos must protect pupils' anonymity and should never show their full face.
- Online photographs and videos of pupils are restricted to the use of side profiles, back of head, or close up images of individual features only.

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to other members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- Use AI-generated content to impersonate others
- Create or share manipulated media involving pupils or staff

The school's use of social media for professional purposes will be checked regularly by the Principal to ensure compliance with the school/Trust policies.

10. Online Safety Infringements & Sanctions

10.1Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

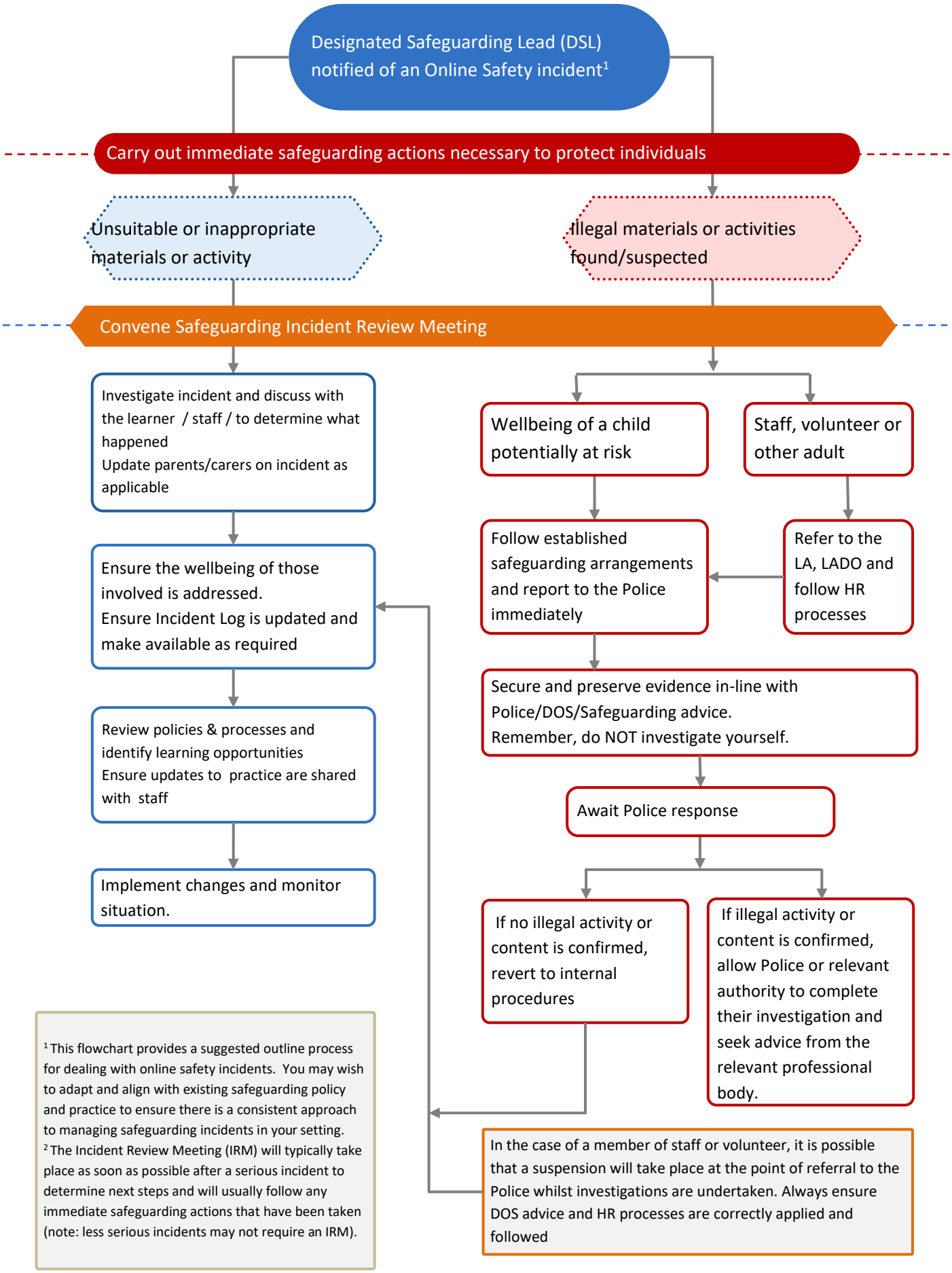
User Actions Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
Pornography				X	
Promotion of any kind of discrimination				X	
threatening behaviour, including promotion of physical violence or mental harm				X	
Promotion of extremism or terrorism				X	
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
Online gaming (educational)			X		
Online gaming (non-educational)				X	
Online gambling				X	
Online shopping / commerce		X			
File sharing			X		
Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting e.g. Youtube		X			

10.2Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

10.3Illegal incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



[1] This flowchart provides a suggested outline process for dealing with online safety incidents. You may wish to adapt and align with existing safeguarding policy and practice to ensure there is a consistent approach to managing safeguarding incidents in your setting.
[2] The Incident Review Meeting (IRM) will typically take place as soon as possible after a serious incident to determine next steps and will usually follow any immediate safeguarding actions that have been taken (note: less serious incidents may not require an IRM).

10.4School / Teaching School / SCITT / Trust Offices Actions & Sanctions

10.4.1 Students/Pupils Incidents

It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures with the appropriate action(s)/sanction(s), as listed below which will be dependent on the nature of the incident and could include a combination of any of the following:

- Refer to class teacher / tutor
- Refer to Head of Department / Year / other
- Refer to Headteacher / Principal
- Refer to Police
- Refer to technical support staff for action re filtering / security etc.
- Inform parents / carers
- Removal of network / internet access rights
- Warning
- Further sanction e.g. detention

Examples of Students / Pupils Incidents could include but are not limited to the following:

- Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).
- Unauthorised use of non-educational sites during lessons
- Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device
- Unauthorised / inappropriate use of social media / messaging apps / personal email
- Unauthorised downloading or uploading of files
- Allowing others to access school network by sharing username and passwords
- Attempting to access or accessing the school network, using another student's / pupil's account
- Attempting to access or accessing the school network, using the account of a member of staff
- Corrupting or destroying the data of other users
- Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
- Continued infringements of the above, following previous warnings or sanctions
- Actions which could bring the school into disrepute or breach the integrity of the ethos of the school
- Using proxy sites or other means to subvert the school's filtering system
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive or pornographic material
- Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act

10.4.2 Staff Incidents

It is intended that incidents of misuse will be dealt with through disciplinary procedures with the appropriate action(s)/sanction(s), as listed below which will be dependent on the nature of the incident and could include a combination of any of the following:

- Refer to line manager
- Refer to Headteacher Principal
- Refer to Local Authority / HR
- Refer to Police
- Refer to Technical Support Staff for action re filtering etc.
- Warning
- Suspension
- Disciplinary action

Staff Incidents could include but are not limited to the following:
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).

- Inappropriate personal use of the internet / social media / personal email
- Unauthorised downloading or uploading of files
- Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account
- Careless use of personal data e.g. holding or transferring data in an insecure manner
- Deliberate actions to breach data protection or network security rules
- Corrupting or destroying the data of other users or causing deliberate damage to hardware or software
- Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
- Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils
- Actions which could compromise the staff member's professional standing
- Actions which could bring the school into disrepute or breach the integrity of the ethos of the school
- Using proxy sites or other means to subvert the school's filtering system
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive or pornographic material
- Breaching copyright or licensing regulations
- Continued infringements of the above, following previous warnings or sanctions

11. Appendix 1 - Online Safety Infringements and Sanctions

11.1Online Safety Infringements and Sanctions

PUPIL	
Category A infringements	Possible Sanctions:
• Use of non-educational sites during lessons • Unauthorised use of email • Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends • Use of unauthorised instant messaging / social networking sites	• Refer to class teacher / tutor • Escalate to: • Phase Leader/RB2L Officer/DSL
Category B infringements	Possible Sanctions:
• Continued use of non-educational sites during lessons after being warned • Continued unauthorised use of email after being warned • Continued unauthorised use of mobile phone (or other new technologies) after being warned • Continued use of unauthorised instant messaging services, social networking platforms, chatrooms or online communities, including TikTok, Snapchat, Discord, Telegram, WhatsApp or similar services. • Use of File sharing software, peer-to-peer services or unauthorised content sharing platforms, includinge.g. BitTorrent or simmilar applications. • Use of anonymous messaging services or applications designed to conceal a user's identity. • Using artificial intelligence tools, AI chatbots, AI image generators, deepfake applications or similar technologies in a manner that breaches the school's acceptable use expectations. • Attempting to access, create or share manipulated, AI-generated or inappropriate content. • Trying to buy items over online	• Refer to Class teacher • Escalate to: • Phase Leader/RB2L Officer/DSL • removal of Internet access rights for a period / removal of phone until end of day / contact with parent

• Accidentally corrupting or destroying others' data without notifying a member of staff of it • Accidentally accessing offensive material and not logging off or notifying a member of staff of it	
Category C infringements	Possible Sanctions:
• Deliberately corrupting or destroying someone's data, violating privacy of others or posts inappropriate messages, videos or images on a social networking site. • Sending an email or message via social networking platforms, chatrooms or online communities, including TikTok, Snapchat, Discord, Telegram, WhatsApp Channels or similar services that is regarded as harassment or of a bullying nature (one-off) • Trying to access offensive or pornographic material (one-off) • AI Generated offensive or harmful images including sexualised images, gender based harm images, offensive images etc. • Deepfake content • Sextortion • AI assisted bullying • Purchasing or ordering of items online • Transmission of commercial or advertising material • Continued sending of emails or regarded as harassment or of a bullying nature after being warned • Deliberately creating accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent • Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988 • Bringing the school name into disrepute	• Refer to Class • Learning Platform access rights for a period • Escalate to: • Phase leader/RB2L Officer/DSL • Principal • contact with parents / removal of equipment • Other safeguarding actions • if inappropriate web material is accessed: • Ensure appropriate technical support filters the site • Refer to Principal / Contact with parents • Other possible safeguarding actions: • Secure and preserve any evidence • Inform the sender's e-mail service provider. • Liaise with relevant service providers/ instigators of the offending material to remove • Report to Police / CEOP where child abuse or illegal activity is suspected

(How will infringements be handled? If the Online-Safety Policy has been infringed, the final decision on the sanction is with the school's senior management.)

STAFF	
Category A infringements (Misconduct)	Possible Sanctions:
• Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc. • Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored. • Not implementing appropriate safeguarding procedures. • Any behaviour on the World Wide Web that compromises the staff members professional standing in the school and community. • Misuse of first level data security, e.g. wrongful use of passwords. • Breaching copyright or license e.g. installing unlicensed software on network.	• Referred to line manager / Principal • Escalate to: Network manager / Online-Safety Coordinator • Warning given
Category B infringements (Gross Misconduct)	Possible Sanctions:
• Serious misuse of, or deliberate damage to, any school / Council computer hardware or software; • Any deliberate attempt to breach data protection or computer security rules; • Deliberately creating, accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent; • Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988; • Uploading confidential information into AI platforms. • Creating AI-generated content involving pupils. • Use of deepfake technology involving members of the school community. • Failure to report AI-generated safeguarding concerns. • Communicating with a pupil via non-school email or social networking platforms, chatrooms or online communities, including TikTok, Snapchat, Discord, Telegram, WhatsApp Channels or similar services	• Referred to Principal / Governors; • Other safeguarding actions: • Remove the PC to a secure place to ensure that there is no further access to the PC or laptop. • Instigate an audit of all ICT equipment by an outside agency, such as the school's ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school. • Where criminal activity is not suspected Identify the precise details of the material. • Escalate to: • report to LA, LADO, LSCPB, Personnel, Human resource.

• Bringing the school name into disrepute	• Report to Police / CEOP where child abuse or illegal activity is suspected.
If a member of staff commits an exceptionally serious act of gross misconduct The member of staff should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken. The school are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.	
Child abuse images found In the case of Child abuse images being found, the member of staff should be **immediately suspended** and the Police should be called. Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP): http://www.ceop.gov.uk/reporting_abuse.html	

How will staff and students be informed of these procedures?

- They will be fully explained and included within the school's online-safety acceptable use agreement form;
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop unacceptable behaviours.
- Pupils will sign an age appropriate online-safety / acceptable use agreement form;
- The school's online-safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the school.
- Information on reporting abuse / bullying etc. will be made available by the school for pupils,