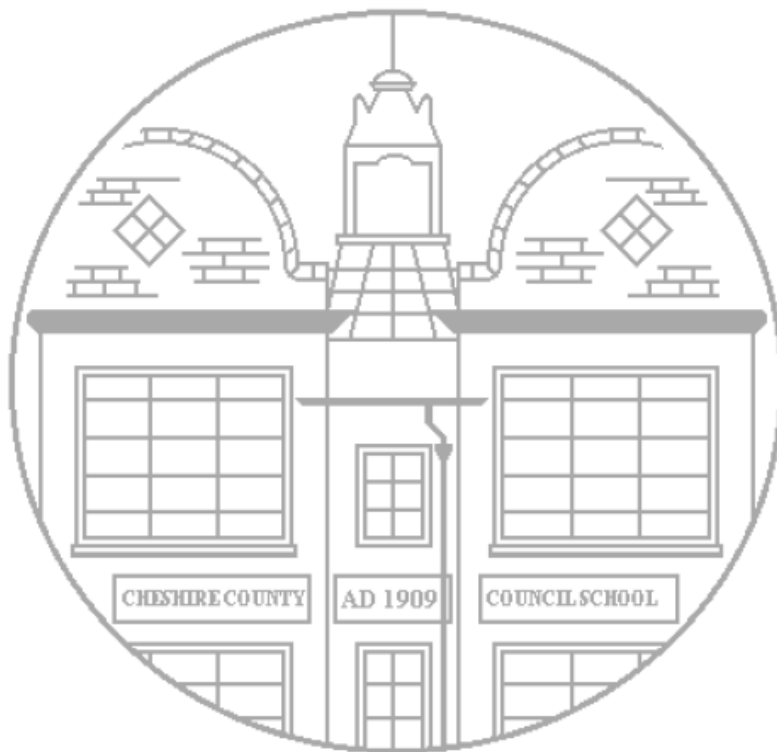


**Cambridge Road
Community Primary & Nursery School**



Online Safety Policy

Approved by: Heather Berry

Date: September 2026

Review date: September 2027

1. Introduction

Cambridge Road Community Primary and Nursery School recognises that technology is an important part of children's education, communication and everyday lives. The school is committed to providing a safe and secure digital environment in which pupils can learn, explore and develop the knowledge and skills they need to use technology responsibly. Online safety is an essential part of safeguarding. It applies to pupils, staff, governors, volunteers, parents/carers and visitors and covers the use of school and personal technology both within and, where relevant, outside school.

This policy should be read alongside the school's:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- Data Protection and Privacy Policy
- Acceptable Use Agreements
- Staff Code of Conduct
- Image Consent arrangements
- Searching, Screening and Confiscation procedures
- Complaints Policy
- Cyber Security arrangements
- Curriculum and Relationships, Sex and Health Education policies.

2. Rationale

The school aims to:

- provide robust processes to protect pupils, staff, volunteers and governors when using technology;
- promote safe, responsible and positive use of technology;
- educate pupils about the benefits, opportunities and risks associated with being online;
- develop pupils' digital resilience and ability to manage online risks;
- provide effective filtering and monitoring systems;
- establish clear procedures to identify, report, investigate and escalate online safety concerns;
- ensure staff understand their safeguarding responsibilities in relation to online activity;
- work in partnership with parents/carers to promote children's online safety;
- respond appropriately to online bullying, harassment, abuse, exploitation and other harmful online behaviour.

Online safety includes the use of the internet, websites, search engines, social media, gaming platforms, messaging services, email, mobile phones, tablets, computers, video conferencing, online learning platforms and artificial intelligence (AI).

The school recognises that technology and online risks change rapidly. This policy will therefore be reviewed regularly and updated when significant changes in technology, safeguarding risks, legislation or national guidance occur.

3. Legal and Policy Framework

This policy has regard to the Department for Education's statutory guidance **Keeping Children Safe in Education 2026 (KCSIE 2026)**, which came into force on 1 September 2026. KCSIE makes clear that safeguarding is everyone's responsibility and that staff must act promptly when concerns arise, including concerns relating to online harms.

The policy also has regard to relevant Department for Education guidance, including:

- *Meeting Digital and Technology Standards in Schools and Colleges – Filtering and Monitoring*
- *Cyber Security: Core Standard*
- *Searching, Screening and Confiscation*
- *Preventing and Tackling Bullying*
- guidance on online safety
- guidance on generative artificial intelligence in education
- *Generative AI: Product Safety Standards*.

The school's processing of personal data will comply with the **UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other applicable data protection legislation**, including relevant provisions introduced by the Data (Use and Access) Act 2025. The school will also have regard to relevant equality and safeguarding legislation and guidance.

4. Roles and Responsibilities

4.1 Governing Body

The Governing Body has strategic oversight of online safety, filtering and monitoring.

The Governing Body will:

- ensure that appropriate online safety arrangements are in place;
- receive appropriate assurance about the effectiveness of filtering and monitoring;
- ensure that online safety is considered as part of safeguarding arrangements;
- ensure that appropriate resources and training are available;
- ensure that filtering and monitoring arrangements are reviewed at least annually;
- appoint a governor with responsibility for oversight of online safety and filtering/monitoring.

Online Safety Governor: Mrs Sass

4.2 Headteacher and Senior Leadership Team

The Headteacher and Senior Leadership Team are responsible for ensuring that this policy is implemented effectively.

They will:

- ensure that online safety is integrated into whole-school safeguarding arrangements;
- ensure appropriate filtering and monitoring systems are in place;
- oversee reports and concerns arising from filtering and monitoring;
- ensure staff receive appropriate training;
- ensure significant incidents are appropriately recorded and acted upon;
- ensure that the school works with external agencies where necessary;
- ensure that the school's online safety arrangements are reviewed regularly.

The DfE's current filtering and monitoring standard requires clear allocation of responsibilities between governors, senior leaders, the DSL and IT support.

4.3 Designated Safeguarding Lead

Designated Safeguarding Lead: Mrs Donna Wellings

The DSL will:

- lead on safeguarding concerns arising from online activity;
- respond to concerns identified through filtering and monitoring;
- ensure online safety concerns are recorded appropriately;
- ensure concerns are managed in accordance with safeguarding procedures;
- make referrals to children's social care, the police or other agencies where appropriate;
- provide governors with assurance that filtering and monitoring arrangements are operating effectively;
- work closely with IT support, senior leaders and the Computing/Online Safety Lead.

The DSL will ensure that staff understand that online safeguarding concerns must be reported without delay. KCSIE 2026 states that staff should act immediately on safeguarding concerns and report them to the DSL or deputy.

4.4 Computing/Online Safety Lead

Computing/Online Safety Lead: Mrs Halhead

The Computing/Online Safety Lead will:

- support the development of online safety education;
 - ensure online safety is incorporated appropriately into the curriculum;
 - support staff with online safety matters;
 - contribute to policy development and review;
 - promote appropriate and responsible use of technology;
 - work with the DSL and IT support when online safety concerns arise.
-

4.5 IT Support / ICT Technician

The school's IT provider/technician has technical responsibility for maintaining filtering and monitoring systems.

They will:

- maintain filtering and monitoring systems;
- provide appropriate reports;
- investigate technical failures;
- ensure filtering and monitoring systems operate on school-managed devices;
- work with the DSL and senior leadership when safeguarding concerns are identified;
- support testing of new devices and services;
- ensure technical changes are appropriately authorised and recorded.

The DfE states that technical responsibility should sit with in-house or third-party IT support working closely with senior leaders and the DSL.

5. Staff and Volunteers

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

- reading and understanding this policy;
- following the school's Acceptable Use Agreement and relevant policies;
- modelling appropriate online behaviour;
- supervising pupils appropriately when they use technology;
- reporting online safety concerns promptly;
- knowing how filtering and monitoring concerns are reported;
- reporting any failure or suspected failure of filtering or monitoring;
- not attempting to bypass filtering or monitoring without appropriate authorisation;
- protecting passwords and account information;
- maintaining professional boundaries when communicating digitally with pupils and parents/carers;
- reporting cyberbullying, online abuse, inappropriate content or safeguarding concerns to the DSL;
- completing required safeguarding and online safety training.

Staff should maintain an attitude of "**it could happen here**", consistent with KCSIE 2026.

6. Parents and Carers

Parents/carers are expected to:

- support the school's approach to online safety;
- encourage their children to use technology responsibly;
- discuss online safety with their children;
- report concerns to the school where appropriate;
- inform the school of significant online incidents affecting their child where these may affect the child's welfare or education;
- follow the school's procedures when communicating digitally with staff.

The school will provide parents/carers with information and guidance about online safety where appropriate.

7. Visitors and Community Users

Visitors and members of the community who are permitted to use the school's ICT systems or internet connection will be informed of relevant expectations and must comply with the school's acceptable-use and safeguarding requirements.

8. Internet Access

Pupils will have supervised and appropriately managed access to the internet as part of their education.

The school will:

- provide appropriate supervision;
- use filtering and monitoring systems;
- teach pupils how to identify reliable and unreliable online information;
- teach pupils how to respond to inappropriate or harmful content;
- ensure pupils know how to report concerns;
- regularly remind pupils about responsible internet use.

If a pupil or member of staff encounters unsuitable content, this should be reported promptly to an appropriate member of staff and, where necessary, the DSL or IT support.

9. Filtering and Monitoring

The school recognises that filtering and monitoring are important safeguarding measures.

The DfE's current standard distinguishes between:

- **filtering**, which is preventative and blocks access to illegal, inappropriate or harmful content; and
- **monitoring**, which identifies and reports activity that may require investigation or safeguarding action.

The school currently uses:

Internet provider: Local Government internet service

Filtering/monitoring system: [Confirm whether Netsweeper, Smoothwall or both are currently used]

The school must confirm the current technical arrangements before this policy is approved.

The school will ensure that:

- filtering is active and appropriately configured;
- monitoring arrangements are proportionate to the school's safeguarding needs;
- staff and pupils are informed that school devices and networks are monitored;
- safe-search settings are appropriately configured;
- filtering and monitoring operate on school-managed devices;
- filtering and monitoring arrangements are reviewed at least annually;
- new devices and services are checked before being made available to pupils;
- filtering and monitoring concerns are recorded;
- high-risk safeguarding alerts are escalated immediately;
- filtering and monitoring failures are reported promptly.

The DfE's current standard requires an annual review involving senior leadership, the DSL, IT support and the responsible governor, with the results and actions recorded. It also expects monitoring plans to include weekly monitoring reports and immediate reporting of high-risk incidents.

10. Filtering Exceptions

Staff must not attempt to circumvent or disable filtering systems.

Where a website or service is required for legitimate educational purposes but is blocked, staff should contact the IT technician/provider.

Any temporary exception must be:

- necessary for an identified educational purpose;
- appropriately authorised;
- time-limited where appropriate;
- recorded;
- reviewed afterwards.

The DfE standard requires temporary exceptions to filtering and monitoring to be approved and documented by the appropriate senior leader. **GGOV.UK**

11. Monitoring Plan

The school's monitoring arrangements will include:

- classroom supervision by staff;
- technical monitoring of school-managed devices and networks where available;
- review of relevant monitoring reports;
- escalation of high-risk alerts;
- recording of actions and outcomes.

Monitoring reports will be reviewed regularly and, as a minimum, the school will ensure that the arrangements meet the DfE requirement for **weekly monitoring reports highlighting incidents**, together with immediate escalation of high-risk incidents.

Records should identify, where available:

- the user;
- device;
- date and time;
- search term/content;
- concern identified;
- action taken;
- outcome.

Monitoring information will be handled in accordance with the school's data protection arrangements.

12. Data Protection and Privacy

The school will comply with the UK GDPR, Data Protection Act 2018 and other applicable data protection legislation.

Personal data will be:

- collected lawfully and transparently;
- used only for appropriate purposes;
- kept accurate where necessary;
- protected from unauthorised access;
- retained only for appropriate periods;
- securely disposed of when no longer required.

The school will consider data protection requirements when introducing new digital systems, monitoring tools or AI products.

Where appropriate, the school will complete a **Data Protection Impact Assessment (DPIA)** and review the privacy arrangements of third-party providers.

The DfE specifically identifies DPIAs and provider privacy notices as relevant to technical monitoring systems.

13. Cyber Security

The school recognises that cyber security is an important part of safeguarding and protecting school operations.

Staff must:

- use strong passwords;
- keep passwords confidential;

- not share accounts;
- report suspicious emails or messages;
- avoid clicking suspicious links or opening unexpected attachments;
- report lost or stolen devices;
- follow school procedures for accessing and storing personal data;
- only install or use authorised software;
- follow IT security instructions.

The school will maintain appropriate security measures, including antivirus/endpoint protection, security updates, access controls, backups and other measures appropriate to its risk profile.

The DfE identifies cyber security as one of the core digital and technology standards for schools.

14. Social Media and Online Communication

Pupils will be taught:

- not to share personal information unnecessarily;
- not to disclose their address, school location or other identifying information to strangers;
- to use strong passwords;
- to use privacy and security settings appropriately;
- not to accept invitations or communicate with unknown people;
- how to block and report unwanted contact;
- how to respond to inappropriate content;
- the importance of age restrictions;
- that online communication can have real-world consequences.

The school will educate pupils about the risks associated with social networking, online gaming, messaging applications and other interactive services.

15. Mobile Phones and Personal Devices

Pupils may only bring mobile phones to school where this has been permitted by the school.

Where permitted:

- phones must be switched off or appropriately secured;
- phones must be stored safely for the school day in accordance with school arrangements;
- pupils must not use personal phones during lessons, break or lunchtime unless specifically authorised;
- pupils must not take photographs, videos or recordings of others without appropriate permission;
- misuse of personal devices will be managed under the Behaviour Policy and, where appropriate, safeguarding procedures.

Staff must follow the school's Staff Code of Conduct regarding personal mobile phones.

16. iPads and School Devices

iPads and other school devices will be used to support teaching and learning.

The school will:

- use devices for planned educational activities;
 - apply appropriate restrictions and filtering;
 - maintain devices securely;
 - ensure devices are stored safely when not in use;
 - ensure software and security updates are applied;
 - monitor appropriate use;
 - ensure pupils understand the school's Acceptable Use Agreement.
-

17. School Website

The school website will contain appropriate school information and contact details.

The school will not publish personal information about pupils or staff unless there is a lawful basis and appropriate permission/arrangement for doing so.

Photographs and other images of pupils will only be used in accordance with the school's image consent arrangements and data protection requirements.

The Headteacher has overall responsibility for the website. Authorised members of staff may contribute content in accordance with school procedures.

18. Email and Digital Communication

The school's official email systems should be used for professional school communication.

Staff must ensure that digital communication with pupils, parents/carers and colleagues is:

- professional;
- appropriate;
- respectful;
- necessary;
- consistent with the Staff Code of Conduct.

Staff must not use personal email accounts to communicate with pupils or for inappropriate school business.

Any email or electronic communication that is threatening, abusive, offensive, inappropriate or concerning must be reported.

Pupils will be taught appropriate email etiquette and how to respond to unwanted or inappropriate communication.

19. Artificial Intelligence

The school recognises that generative AI can provide educational opportunities but can also introduce risks relating to safeguarding, inappropriate content, misinformation, privacy, data protection, intellectual property and harmful or manipulative content.

The school will assess AI products before approving them for use.

The DfE's current AI product safety standards identify requirements around filtering, security, privacy, intellectual property, governance and child safety.

Staff

Staff must:

- only use AI tools approved by the school where required;

- not enter confidential, sensitive or personal pupil information into an unapproved AI tool;
- check AI-generated content for accuracy and suitability;
- consider copyright and intellectual property;
- maintain professional judgement and responsibility for decisions;
- follow the school's data protection requirements;
- report AI-related safeguarding concerns.

Pupils

Pupils will only use AI tools where permitted by the school and under appropriate supervision.

Pupils will be taught that:

- AI-generated information may be inaccurate;
- AI does not replace teachers or trusted adults;
- they must not share personal or confidential information with AI tools;
- they must not use AI to bully, threaten, impersonate or harm another person;
- they must not create or share harmful, sexualised or abusive AI-generated material;
- they must report concerning AI-generated content to an adult.

The school will treat AI-generated bullying, harassment, sexualised imagery, manipulated images, audio or video and other harmful material as a safeguarding and/or behaviour concern as appropriate.

20. Cyberbullying

Cyberbullying includes harmful behaviour carried out using digital technologies such as:

- social networking;
- messaging applications;
- gaming platforms;
- email;
- online discussion forums;
- video-sharing platforms;
- group chats.

Cyberbullying may involve repeated behaviour and an imbalance of power, but the school recognises that a single serious online incident may also constitute a safeguarding, harassment, sexual harassment or criminal concern.

The school will:

- teach pupils what cyberbullying is;
- teach pupils how to report concerns;
- encourage pupils to report concerns affecting themselves or others;
- provide appropriate support to pupils affected;
- work with parents/carers;
- record significant incidents;
- use the Behaviour Policy and safeguarding procedures where appropriate.

Where illegal or potentially illegal material is involved, the school will seek advice from the DSL and relevant external agencies, including the police where appropriate.

21. Online Sexual Harassment and Harmful Sexual Behaviour

The school recognises that sexual harassment and harmful sexual behaviour can occur online as well as offline.

Concerns may include:

- sexualised messages;
- unwanted sexual communication;
- requests for intimate images;
- sharing intimate images;
- threats to share images;
- manipulated or AI-generated sexual images;
- sexualised group-chat behaviour;
- sexual harassment through gaming or social media.

All such concerns will be treated seriously and managed in accordance with the school's safeguarding and child protection procedures.

Staff must report concerns to the DSL without delay.

22. Online Grooming and Exploitation

Pupils will be taught that people online may not always be who they claim to be.

The school will teach pupils:

- not to meet online contacts in person;
- not to share personal information;
- not to send photographs or videos to strangers;
- how to block and report unwanted contact;
- how to recognise manipulation and grooming;
- how to seek help from a trusted adult.

Any concern that a child may be experiencing grooming, exploitation or abuse will be managed under the school's safeguarding procedures.

23. Searching and Electronic Devices

Where a search of a pupil or electronic device is necessary, staff will follow the school's Behaviour Policy and current Department for Education guidance on **Searching, Screening and Confiscation**.

Staff will not routinely search or delete material from a pupil's device outside the school's agreed procedures.

Any safeguarding concern identified during a search will be reported to the DSL.

24. Online Safety Curriculum

Online safety will be taught as part of the curriculum and reinforced throughout the school year.

Teaching will include age-appropriate material covering:

- safe internet use;
- privacy;
- passwords;
- personal information;

- online relationships;
- online communication;
- cyberbullying;
- online gaming;
- social media;
- misinformation and unreliable content;
- online advertising;
- image sharing;
- sexual harassment and harmful content;
- online grooming and exploitation;
- digital footprints;
- artificial intelligence;
- reporting and blocking;
- digital resilience.

The school will provide additional teaching and support where emerging risks are identified.

25. Acceptable Use Agreement – Key Stage 1

I will:

- use school computers and technology sensibly;
- only use the internet when a teacher or adult says I can;
- use my own username and password;
- keep my password private;
- look after school equipment;
- only look at my own work;
- ask before using a USB or other device from home;
- tell an adult if I see something that worries, upsets or frightens me;
- keep personal information private;
- tell an adult if someone online makes me uncomfortable;
- understand that school may monitor my use of school technology;
- follow the school's rules when using technology.

If I do not follow these rules, I understand that I may lose access to school technology and other appropriate action may be taken.

26. Acceptable Use Agreement – Key Stage 2

I will:

- use school computers and technology sensibly;
- ask permission before using the internet;
- only use my own username and password;
- keep my password confidential;
- only access my own work;
- not delete or change another person's files;
- not bring USB devices or other storage devices from home without permission;
- only use email and messaging services as directed by a member of staff;
- use polite and appropriate language;

- not give out personal information;
- not arrange to meet someone I have only met online;
- tell an adult if someone online makes me uncomfortable;
- tell an adult if I see something online that worries, upsets or frightens me;
- not use AI tools unless a member of staff has given permission;
- not use technology to bully, threaten, embarrass or harm another person;
- not create or share inappropriate images or content;
- understand that school technology may be monitored;
- follow the school's online safety rules.

If I do not follow these rules, I understand that I may lose access to school technology and other appropriate action may be taken.

27. Reporting an Online Safety Concern

Pupils should tell a trusted adult if:

- something online makes them uncomfortable;
- someone asks them to keep an online secret;
- someone they do not know contacts them;
- they receive an inappropriate message or image;
- they are bullied online;
- someone threatens them;
- someone asks for personal information or photographs;
- they see harmful or illegal content;
- they are worried about something another pupil has done online.

Staff should report concerns promptly to the DSL or another appropriate member of staff. Staff should not delay reporting a safeguarding concern while attempting to investigate it themselves.

28. Online Safety Incident Management

Significant incidents will be:

1. reported to the DSL or appropriate senior member of staff;
2. recorded appropriately, including on CPOMS where required;
3. assessed for safeguarding, behaviour, data protection and/or criminal implications;
4. escalated to parents/carers where appropriate;
5. referred to external agencies where necessary;
6. reviewed to identify whether further education, support or changes to systems are required.

Records should include:

- the concern;
- date and time;
- people involved;
- action taken;
- decisions made;
- rationale for decisions;
- outcome.

This reflects the recordkeeping expectations set out in KCSIE 2026.

29. Complaints

Complaints concerning online safety will be managed in accordance with the school's Complaints Policy and relevant safeguarding procedures.

Complaints involving:

- pupil online behaviour will normally be managed under the Behaviour Policy and safeguarding procedures where appropriate;
 - staff misuse will be referred to the Headteacher and managed in accordance with the relevant staff/safeguarding procedures;
 - child protection concerns will be referred immediately to the DSL;
 - technical or filtering concerns will be referred to IT support and the appropriate senior leader.
-

30. Staff Training

All staff will receive appropriate online safety and safeguarding training.

Training will include, where relevant:

- online safeguarding;
- filtering and monitoring;
- cyberbullying;
- online sexual harassment;
- image sharing;
- grooming and exploitation;
- AI-related risks;
- data protection;
- cyber security;
- phishing and malicious communications;
- reporting procedures;
- professional online communication.

The DfE provides current training materials specifically addressing safeguarding, data, ethics and intellectual-property risks associated with generative AI.

31. Parent/Carer Information

The school will provide parents/carers with information about online safety through appropriate channels, which may include:

- newsletters;
- school meetings;
- information leaflets;
- the school website;
- workshops;
- signposting to reputable online safety resources.

Parents/carers will be encouraged to discuss online safety regularly with their children.

32. Communication of this Policy

This policy will be:

- available to staff;
- available to parents/carers;
- available through the school website where appropriate;
- referenced in relevant safeguarding documentation;
- communicated to pupils through age-appropriate teaching;
- supported by Acceptable Use Agreements.

Pupils will be informed that their use of school technology and networks may be filtered and monitored.

33. Risk Assessment

The school recognises that no filtering system can guarantee that all inappropriate content will be blocked.

The school will therefore use a combination of:

- filtering;
- monitoring;
- supervision;
- education;
- staff training;
- acceptable-use agreements;
- safeguarding procedures;
- appropriate technical security measures.

The school will regularly assess emerging online risks and take reasonable and proportionate steps to reduce them.

The DfE's current filtering standard specifically recognises that no filtering system is 100% effective and requires schools to understand limitations and mitigate associated risks.

34. Annual Review of Online Safety, Filtering and Monitoring

The school will review this policy and its online safety arrangements at least annually.

The filtering and monitoring review will involve:

- a member of the Senior Leadership Team;
- the DSL;
- IT support/provider;
- the Online Safety/Computing Lead;
- the responsible governor.

The review will consider:

- current filtering arrangements;
- current monitoring arrangements;
- safeguarding incidents;
- monitoring reports;
- emerging online risks;
- use of AI;
- new devices and applications;
- staff and pupil feedback;

- SEND and accessibility considerations;
- data protection;
- cyber security;
- effectiveness of staff training;
- curriculum provision;
- any identified gaps.

The outcome of the review will be documented, including actions, responsible persons and timescales. The DfE currently requires filtering and monitoring provision to be reviewed at least annually and records of checks and actions to be maintained.

35. Policy Review

This policy will be reviewed annually or sooner where there is:

- a member of the Senior Leadership Team;
 - the DSL;
 - IT support/provider;
 - the Online Safety/Computing Lead;
 - the responsible governor.
 - a significant change in legislation;
 - a change to KCSIE;
 - a significant change to DfE guidance;
 - a significant safeguarding incident;
 - a change to filtering or monitoring arrangements;
 - introduction of new technology or AI;
 - a significant change to the school's digital infrastructure.
-