Hatch Ride Primary School

All in one E Safety Policy

Published Date:	06/02/2025
Date of Next Review:	05/02/2027
Statutory/Non-Statutory:	Statutory
Public/Internal:	Public
Applies to:	All
Date Approved by Local Governing Body:	06/02/2025

Policy Statement:

This is a School policy that will be adopted by all relevant personnel within the School

Purpose:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or

pornography), sharing other explicit images and online bullying; and

- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Responsibility for Approval:	Local Governing Body
Responsibility for Updating:	School
Related Policies/Guidance:	• Data Protection Act 2018 • General Data Protection Regulation • Staff Acceptable Use Policy • Behaviour policy • Business Continuity Policy/Rainbow Plan • Complaints policy

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study and complies with our funding agreement and articles of association.

1. Roles And Responsibilities

1.1 The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's IT systems and the internet.
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

1.2 The Headteacher & SLT

The headteacher & SLT is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

1.3 The Designated Safeguarding Lead/CPO

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher, IT support and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school child protection policy.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the headteacher and/or governing board

The DSL/CPO should be trained in e-Safety issues and be aware of child protection matters that may arise from:

- Sharing or loss of personal data.
- Access to illegal/inappropriate materials.
- Inappropriate on-line contact with adults/strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.

This list is not intended to be exhaustive.

1.4 IT Support

IT support is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that best practices are implemented to secure and protect against viruses and malware, and that such safety mechanisms are updated regularly.
- Blocking access to potentially dangerous sites when identified and, where possible, preventing the downloading of potentially dangerous files.

This list is not intended to be exhaustive.

1.5 Data Protection Officer

Responsible for maintaining registration with the Information Commissioner's Office, keeping abreast of regulatory requirements and recommendations as outlined on their website at www.ico.gov.uk and informing staff and leadership so that school policies may be updated.

1.6 E-Safety Coordinator

- Takes day-to-day responsibility for e-Safety issues and has a leading role in establishing and reviewing the school e-Safety policies/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place.
- Provides training and advice for staff through staff meetings and briefings, briefings for parent volunteers, LSA meetings.
- Liaises with the Trust and the Local Authority.
- Liaises with the school's IT support.
- Receives reports of e-Safety incidents and creates a log of incidents to inform future e-Safety developments.
- Meets regularly with e-Safety Governor to discuss current issues, review incident logs and filtering/change control logs.
- Attends relevant committee meetings of Governors.
- Reports regularly to the Senior Leadership Team.
- Provide materials and advice for integrating e-Safety within PSHE and ICT schemes of work.
- Check that e-Safety is taught on a regular basis.

This list is not intended to be exhaustive.

1.7 All Staff and Volunteers

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

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's IT systems and the internet and ensuring that pupils follow the school's terms on acceptable use.

- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

1.8 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's IT systems and internet.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

1.9 Visitors And Members of The Community

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

2. Educating Pupils About Online Safety

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

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

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

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.

- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

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

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

3. Educating Parents About Online Safety

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

Online safety will also be covered during parents' evenings.

The school will let parents know:

- What systems the school uses to filter and monitor online use.
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

4. Cyber-Bullying

4.1 Definition

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

4.2 Preventing And Addressing Cyber-Bullying

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

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

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

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

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

4.3 Examining Electronic Devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Assess how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- Seek the pupil's cooperation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image.
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

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

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

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

5. Acceptable Use of The Internet in School

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

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

6. Use Of Mobile Devices in School

- Pupils are not allowed to bring mobile phones to school unless prior arrangements are made with the school. If required, then the child is to have them signed in and out and the teacher will place in a lockable storage unit.
- Pupils are not allowed to bring in games devices.
- Teacher/parent contact should normally be by the main school telephone, office email or other communication methods setup and managed by the school (and not via a mobile device except where off-site activities dictate the use of mobile phone).
- Parent helpers in school and staff must ensure that they do not send personal messages, either audio or text, during contact time with pupils. If an exceptional emergency arises they should arrange temporary cover whilst they make a call.
- Staff, helper and visitor mobile devices should be switched off or on silent during the times that children are present.
- No device in any of the school buildings should contain any content that is inappropriate or illegal.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

7. Local Network Security

- The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented by those responsible.
- Physical access to servers and communications cabinets is restricted.
- All users will have clearly defined access rights to school IT systems.
- Critical passwords for the school IT system in addition to being known by IT support will be securely stored and accessible only to the head teacher/deputy head teacher.
- All staff have an individual password (see password protocol).
- No individual should log on using another individual's password, unless they are a member of staff logging on as a child.
- Pupils may have a group password or be given individual passwords for accessing the network.
- The school's IT support may monitor and record the activity of users on the school IT systems and users are made aware of this through the Acceptable Use Policy.
- A separate segregated guest network shall be maintained which is to be used by all devices not owned by the school.

8. Internet Security (Including Web Access)

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to

guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

- The school maintains and supports the managed filtering service provided by a 3rd party organisation. Any filtering issues are to be reported immediately to the 3rd party.
- Periodically the filtering service may be reviewed and/or changed. Due diligence must take place prior to any changes to ensure it meets the goals and requirements of this policy and any applicable legislation.
- All Pupils using the World Wide Web must be made aware of the school's NetSmart Code. These should be posted near to the computer systems.
- Instruction in responsible and safe use will precede Internet access on a regular basis (at least once each term).
- Pupils and staff will be informed that Internet access will be monitored.
- The school will audit IT provision to establish if the e-Safety policy is adequate and that its implementation is effective.
- Course of action if inappropriate content is found (i.e. that is pornographic, violent, sexist, racist or horrific)

1. **The user should:**
    1.1. Turn off the monitor or minimise the window.
    1.2. Report the incident to the teacher or responsible adult.
2. **The teacher should:**
    2.1. Ensure the well-being of the pupil.
    2.2. Note the details of the incident, especially the web page address that was unsuitable (without re-showing the page to the pupils).
    2.3. Report the details of the incident to the e-Safety officer.
3. **The e-Safety officer will then:**
    3.1. Log the incident and take any appropriate action.

- Where necessary report the incident to the Internet Service Provider.

9. School Password Protocol

All passwords used by adults should follow the guidelines in this policy.

- No individual should tell another individual their password.
- Once a computer has been used, users must remember to log off so that others cannot access their information. Users leaving a computer temporarily should lock the screen.
- Passwords must not be easily guessable by anyone and should follow NCSC guidance on selecting secure passwords (guidance can be found at the time of writing here: https://www.ncsc.gov.uk/collection/passwords/updating-your-approach#tip5-password-collection
- Passwords must be unique and not used for any other service (e.g. a user's personal email).
- Should a user know their password is insecure and/or has been compromised it is essential that the password is changed immediately.

10. Virus Protection

- All systems (except where technological considerations preclude doing so) are protected by an Antivirus product which is preferably administered centrally and automatically updated.

- Any virus, adware or malware incidents should be reported immediately to IT support.
- Any data received form a 3rd party (such as downloading files from the web) must be scanned by an up-to-date Antivirus product prior to use.
- Memory Sticks, Memory Cards, CDs, and other portable storage must not be used and/or connected to a device unless explicitly confirmed by IT support.
- In line with the above point visitors to the school wishing to use their own digital content at school must either:
    1. Send the content via the internet to the school prior to their visit. It should then be scanned by the school and if no issues are found made available to them upon arrival.
    2. Use their own device which can be connected to the segregated guest network and connected, if required, to a display.

11. Communication Guidance

Including, but not limited to, emails, SMS.

- Staff may not use personal email accounts for any school business.
- Pupils will not have access to school email.
- Pupils may not access personal email accounts whilst in school or whilst using school equipment.
- Teachers' email addresses are not to be included in emails to parents unless they are under BCC.
- Pupils should immediately tell a teacher if they receive an offensive e-mail or message or find an inappropriate web page.
- Pupils should not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone via an e-mail or message.
- The forwarding of chain letters and jokes is prohibited in school.
- 12Pupils may only use approved e-mail or message accounts on the school system.

12. Backing Up of Data

- Data held on individual systems is liable to be overwritten without notice during the process of maintaining the computers. Systems may also fail or be stolen. Staff should therefore ensure no data is stored on the local drive of any client computer unless it’s serving as a local cache to remote backed storage.
- When using a system that uses synchronisation to store data staff must periodically check that the synchronisation is working correctly. IT support can provide guidance how to do this.
- For servers and other critical central systems:
    1. Backups of critical data must be held in a secure location, geographically distant from the school network servers.
    2. Backup logs are checked periodically and a partial recovery from backup is tested termly to ensure the data is usable.
- A whole school ICT disaster recovery plan is part of the Business Continuity Plan found in the Rainbow Plan folder.

13. The School Website

- The school’s website should include the school address, school email, telephone and fax number including the school's emergency email address.
- Staff or Pupils' home information should not be published.

- The copyright of all material posted must be held by the school or be clearly attributed to the owner where permission to reproduce has been obtained or given e.g. via Creative Commons licensing where appropriate.

See Photography of Pupils for detail concerning the use of photographs

14. Staff Using School Devices In and Out of School.

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords (see school password protocol).
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Not sharing the device among family or friends.
- Keeping operating systems, antivirus, and other software up to date by always installing the latest updates. This may require manually running updates from an online source if access to network update services is unavailable due to being off site. Please seek advice from IT support if necessary.
- Devices should be locked when the user leaves their computer.

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

Work devices must be used solely for work activities.

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

In addition to the information above the following security measures should be taken with devices when taken out of school:

- Devices must be out of view and preferably locked away overnight particularly when left at school.
- Devices should never be left in a parked car, even in the boot.
- Nobody outside of the school staff should be allowed to access a school's device.

Loading software

For this policy, software relates to all programs, images or screensavers, which can be downloaded or installed from other media.

- Only IT support, or those acting specifically on their behalf are allowed to load software on to any school computer.
- Images and video clips may be downloaded if the teacher in charge is satisfied that they are not breaching copyright.
- Software loaded on to any school system must be:
    1. Properly licensed.
    2. Free from viruses.

15. School Handling and Security of Personal and Sensitive Data

All data is subject to the school's Data Protection policy.

Personal data is any data which allows an individual to be identified. A name alone does not constitute personal data but a name and an address, or name and date of birth does. Sensitive data is a subset of personal data and includes additional information such as medical information. Examples include:

- SEN records such as ILJs and Annual Review records.
- Marksheets and assessments.

- Reports and Open Evening comments.
- Personal data stored on the School Information Management System, SIMS.
- Photographic or video material.
- Name, address and contact information.
- Non-sensitive or non-personal data thus includes:
    1. General teaching plans.
    2. Curriculum materials.
    3. General correspondence of a non-personal nature.

Using and storing personal and sensitive data:

- All users are responsible for only accessing, altering and deleting their own personal files. They must not access, alter or delete files of another user without permission.

Personal and sensitive data only be stored be on:

- The school network servers.
- A school owned client system when serving as local cache to remote backed storage and when the client system is both encrypted and password protected.
- The school's Microsoft 365 tenant.
- A school email or communication system as part of a communication.
- Other systems explicitly approved by the school/trust DPO.
- No other storage medium is permissible.

Emailing personal and sensitive data:

- Should not be used to email between staff using our school email system. Data should be stored in an appropriate location and a link to the data shared via email.
- Should only be sent to recipients outside the school (e.g. health professional, Local Authority) using the secure email facility.

16. Photography

Photography Of Pupils - General

- Pupils' full names will not be used in conjunction with photographs on the public part of the Learning Platform or school website.
- Only photographs of Pupils whose parents have given permission for them to appear on our Learning Platform or website will be used.
- Photographs of children used on the website are always with another child or in a group.
- Staff will check the Photograph list to ensure that no photograph of a learner without permission is used.
- Names can be used in conjunction with photos on the password protected parts of the Learning Platform.
- Where staff personal devices are being used for school purposes, consideration must be given to the security of Images/data in case of loss of the device e.g. photos should be downloaded in school and removed from the camera or memory card.
- All photographs downloaded to the school network should be placed in All School Photos on the Shared drive.
- Photographs taken by the newspaper have parents' permission to publish names unless included on the Photograph list.

Photography Of Pupils - Parents

- Parents may take photographs of their children during sports events and following any performances, but they should not be posted on social networking sites with permissions set to public.
- Parents' permission for the use of photographs is requested as part of the school induction pack.

Photography Of Pupils - Staff and Pupils

- Only school cameras should be used. If own cameras are needed e.g. on trips, photographs must be downloaded in school immediately on return and removed from own camera.
- All devices capable of taking photographs, whether belonging to the school or personal, may be subject to scrutiny by managers if required.
- It is the staff's responsibility to ensure children without permission are not photographed for any newspaper.

17. Training

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

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

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

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

Training will also help staff:

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

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

18. Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

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

19. Social Media

Staff use of Social Networking

- Staff have a right to use social networking sites.
- Staff should ensure that public comments they make on social networking sites are compatible with their role as a member of staff and that they show the highest standards of professional integrity.
- Staff should not post photographs of any pupils on their personal social networking profile unless there is a legitimate reason for this to be the case. For example:
    1. The staff member is related to the pupils (e.g it is of their child).
    2. The staff member is associated with the pupils outside of their role as a member of staff (e.g. friends with parents).
- Staff should check their profile settings in social networking sites to ensure that:
    1. No pupil (or recent past pupil (under 16)) is able to see extra material that is not public (eg not be a friend or a contact).
    2. No parent of a pupil at school should be able to see extra material that is not public unless there is a legitimate reason for this to be the case for example:
        2.1. The staff member is associated with the parent outside of their role as a member of staff.
        2.2. The staff member has a child at the school and hence access may be appropriate within that context.
    3. Any changes to social networking sites and privacy settings are clearly understood.
- Where members of staff feel they have a legitimate reason, as outlined above, they must disclose this to the head teacher as soon as they aware of the need to do so.

Child use of Social Networking sites

- Pupils will not be allowed to access public or unregulated chat rooms.
- Pupils at school are regularly educated in e-Safety which includes the safe use of social networking sites.

School Social Media Sites

- The school has a Facebook and Twitter Account – monitored and managed by designated staff members.
- These tools are not lines for communication or correspondence but for information only.
- Facebook Parents Page is only for current Parents.

20. Complaints Regarding Internet Use

- Any complaints regarding Internet misuse will be dealt with in accordance with the school Behaviour Policy.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaint's procedure.

21. How The School Will Respond to Issues of Misuse

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

Where a staff member misuses the school's IT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary

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

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

- A system of appropriate sanctions will be used to promote the safe use of technology within school. E.g. Suspension of messaging permissions, individual access to the Learning Platform, school PCs etc.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. This would constitute a disciplinary matter as far as staff are concerned.

22. Parental Support

- Parents will be made aware of the school's policies regarding e-Safety and Internet use through e-Safety meetings, newsletters and the Learning Platform.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet may be made available to parents as appropriate.