



ONLINE SAFETY POLICY



Document Status -

Policy Authors	Hollinswood Primary School & Nursery
Policy Previous Review Date	December 2022
Current Policy Date	September 2026
Policy Review Frequency	Annually
Date of Next Review	September 2027
Committee/Approver of Policy	Full Governing Body

Contents

1. Aims	2
2. Legislation and guidance	3
3. Roles and responsibilities	4
4. Educating pupils about online safety	8
5. Educating parents/carers about online safety	10
6. Cyber-bullying	10
7. Acceptable use of the internet in school	13
8. Pupils using mobile devices in school	13
9. Staff using work devices outside school	14
10. How the school will respond to issues of misuse	15
11. Training	15
12. Monitoring arrangements	16
13. Links with other policies	16
Appendix 1: Acceptable use agreement	17
Appendix 2: online safety training needs – self-audit for staff	21
Appendix 3: online safety incident report log	22

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Identify and support groups of pupils that are potentially at greater risk of harm online than others.
- 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 – Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, misinformation, disinformation, conspiracy theories, 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

2. Legislation and guidance

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](#)

➤ [Relationships and sex education](#)

➤ [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.

This policy also reflects:

- The Online Safety Act 2023, which introduces duties on online platforms to protect children from harmful and illegal online content.
- The Department for Education (DfE) Filtering and Monitoring Standards for Schools and Colleges..

- Guidance relating to the safe use of generative artificial intelligence (AI) within education settings.

The policy also takes into account the National Curriculum computing programmes of study.

The school recognises that online risks continue to evolve and therefore adopts a dynamic approach to online safety, risk assessment and staff training

3. Roles and responsibilities

3.1 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 make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

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

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems.
- Reviewing filtering and monitoring provisions at least annually.
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning.
- Having effective monitoring strategies in place that meet their safeguarding needs.

The school will use the DfE filtering and monitoring review process and self-assessment tools to evaluate effectiveness annually and following any significant safeguarding incident.

Senior leaders, governors and the DSL will understand:

- what filtering systems block;
- what monitoring systems identify;
- the limitations of these systems;
- how safeguarding concerns identified through monitoring are escalated and acted upon.

The governor who oversees online safety is Clare Lo

All governors will:

- Ensure they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (see appendix 1)
- 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.

3.2 The headteacher

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

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) and deputies 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:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT technician/manager and Computing Lead to make sure the appropriate systems and processes are in place.
- Working with the ICT technician/manager, Computing Lead 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's child protection policy
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged on CPOMS and dealt with appropriately in line with the school behaviour policy.
- Ensuring that any incidents of systems or processes failing are acted upon and recorded using incident report (appendix 3).
- 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.
- Undertaking annual risk assessments that consider and reflect the risks children face.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.
- Monitoring emerging risks associated with artificial intelligence and generative AI technologies.
- Ensuring risk assessments are completed before new AI tools or applications are introduced.
- Supporting staff in the safe, ethical and lawful use of AI technologies

This list is not intended to be exhaustive.

3.4 The ICT technician/manager

The ICT technician/manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually 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 the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems on a regular basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 1), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes and being aware of how to report any incidents of those systems or processes failing by reporting directly to the DSL.
- Following the correct procedures by alerting the DSL if they need to bypass the filtering and monitoring systems for educational purposes.
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS 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 and logged on CPOMS.

- 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'.
- Using AI tools in accordance with school guidance and data protection requirements.
- Not inputting personal, sensitive or confidential information into public AI platforms unless authorised risk assessments have been completed.
- Reporting any concerns regarding AI-generated content, deepfakes, misinformation or harmful use of AI technologies

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers 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 ICT systems and internet (appendix 1)

Parents/carers 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](#)
- Parent resource sheet – [Childnet](#)

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 1).

4. Educating pupils about online safety

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

The text below is taken from the [National Curriculum computing programmes of study](#).

It is also taken from the [guidance on relationships education, relationships and sex education \(RSE\) and health education](#).

All schools have to teach:

- [Relationships education and health education](#) in primary schools

Primary schools

In **Key Stage (KS1)**, 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 (KS) 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.

Pupils will also be taught:

how to identify misinformation, disinformation and manipulated content;

how artificial intelligence may generate inaccurate or misleading information;

how to evaluate online sources critically;

how algorithms, influencers and online platforms can shape opinions and behaviour;

how to report harmful, illegal or suspicious online content.

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.

5. Educating parents/carers about online safety

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

The school will let parents/carers 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.

The school will provide regular information to parents and carers relating to:

- emerging online risks and trends;
- social media developments;
- online scams and financial exploitation;
- artificial intelligence applications and associated safeguarding risks;
- age-appropriate use of devices and online services

If parents/carers 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.

6. Cyber-bullying

6.1 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 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.

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/carers so 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.

6.3 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:

- Make an assessment of 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 co-operation.

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/carer 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 [searching, screening 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.

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

6.4 Artificial intelligence (AI)

Artificial Intelligence (AI)

The school recognises that artificial intelligence (AI) technologies are increasingly used by children and adults and may bring both educational benefits and safeguarding risks.

Risks may include:

- creation and sharing of deepfake images, videos or audio;
- AI-generated bullying or harassment;
- misinformation and disinformation;
- grooming or exploitation using AI-generated content;
- inappropriate dependence on AI-generated responses;
- breaches of confidentiality or personal data protection.

Staff must not enter confidential, personal or safeguarding information into publicly available AI systems unless explicitly authorised and risk assessed.

Any suspected misuse of AI technology that places a child at risk will be managed in line with safeguarding procedures and recorded on CPOMS.

The school will risk assess AI tools before use and ensure that any educational AI technology operates alongside existing filtering, monitoring and safeguarding arrangements. [saferinternet.org.uk], [education-...erts.co.uk]

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendix 1). 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 and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendix 1.

8. Pupils using mobile devices in school

Upper KS2 pupils may bring mobile devices into school but these must be stored in the school office and pupils are not permitted to use them during school hours/trips.

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.

9. Staff using work devices outside school

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

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- 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.
- Making sure the device locks if left inactive for a period of time.
- Not sharing the device among family or friends.
- Installing anti-virus and anti-spyware software.
- Keeping operating systems up to date by always installing the latest updates.

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 1.

Work devices must be used solely for work activities.

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

Cyber Security

The school recognises cyber security as an important safeguarding responsibility.

The school will:

- maintain appropriate technical security controls;
- ensure software and systems are regularly updated;
- provide staff awareness training on phishing, social engineering and cyber threats;
- maintain procedures for responding to cyber incidents;
- assess cyber security risks as part of annual safeguarding reviews.

Any cyber incident that may impact safeguarding, confidentiality or access to critical systems will be reported immediately to senior leaders and recorded appropriately.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our 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 ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. 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, and staff meetings).

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

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

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse.
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh 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 and deputies 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.

12. Monitoring arrangements

Staff log behaviour and safeguarding issues related to online safety directly onto CPOMS. The DSL monitors all incidents related to online safety.

An incident report log is used to report any system/processes failing. This log can be found in appendix 3.

This policy will be reviewed annually by the Online Safety Team (DSL, Computing Lead, IT Technician and Link Governor), following publication of the latest KCSIE guidance and whenever significant legislative or technological developments occur.

The review will include:

- filtering and monitoring effectiveness;
- cyber security arrangements;
- AI-related risks;
- emerging online safeguarding risks;
- incident trends and lessons learned;
- the effectiveness of online safety education for pupils, staff and parents/carers.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Mobile and Smart Technology policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: EYFS, KS1, KS2 and staff acceptable use agreement

Online Safety Rules for Foundation Stage

- I will take care of school computing equipment. If I spot any damage, I will tell my teacher.
- I will only use the program or website that my class is working on.

Online Safety Rules for KS1

- I will take care of school computing equipment. If I spot any damage, I will tell my teacher.
- I will only use the program or website that my class is working on.
- I will use my own login and password and will not share my password with my others.
- I will treat other children's work with respect.
- I will tell an adult if I see anything online that I am uncomfortable with.
- I will remember to follow the online safety rules at home.

Online Safety Rules for KS2

- I will take care of school computing equipment. If I spot any damage, I will tell my teacher.
- I will use my own login and password and will not share my password with my others.
- I will not go on inappropriate sites. If I do this accidentally, I will tell my teacher.
- I will tell an adult if I see anything that I am uncomfortable with online.
- I will make sure I am respectful when writing online and will always use positive comments.

- I will make sure I do not copy anyone else's work or information from the internet and pretend it's my own.
- I will remember to follow the online safety rules at home.
- I will only use the names and pictures of my friends if they say it's OK.
- I will only send emails or messages to teachers or to discuss schoolwork.
- Out of school, I know I must not arrange to meet anyone that I don't know.

Acceptable Use Policy for school staff

Any messages, photos, videos or other media I post online will be out of my control. Any inappropriate searches on the internet will be reported to school. I agree that I will not:

- Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
 - pornography (including child pornography)
 - promoting discrimination of any kind
 - promoting racial or religious hatred
 - promoting extremism and radicalisation
 - promoting illegal acts
 - breach any Local Authority/School policies, e.g. gambling
 - do anything which exposes children in my care to danger
 - any other information which may be offensive to colleagues
- Forward chain letters, breach copyright law, do anything which exposes children to danger including, take images of pupils out of the premises on removable media or taking sensitive pupil information off the premises on removable media that is not encrypted

When using ICT equipment, I will not:

- Give anyone access to my login name or password
- Attempt to introduce any unlicensed applications
- Corrupt, interfere with or destroy any other user's information
- Release any personal details of any colleague or pupil over the Internet
- Use the school internet access for business, profit, advertising or political purposes
- Leave my account open at the end of a session – remember to 'lock' the screen

When using email I will:

- Only communicate with pupils, parents/carers and other professionals via a school provided email address or telephone number or via the message function on ClassDojo

- Observe 'network etiquette' on all occasions. Email or messaging should not be considered a private medium of communication and great care should always be taken over content, because of the possibility of public scrutiny
- Make sure that nothing in messages could be interpreted as libellous
- Not send any message which is likely to cause annoyance, inconvenience or needless anxiety

When working on professional documents that contain school-related information I will:

- Ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 2018.
- Not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones or memory sticks), unless they are secured and encrypted
- Protect the devices in my care from unapproved access or theft
- Not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information

When using outside systems, I will:

- Make sure that any information I share on social networking sites takes into account my role as a member of staff
- Not allow pupils to be "friends" with me on social networking sites
- Keep data about students safe and be responsible for ensuring that the data protection act is not breached

This policy applies to both fixed and mobile internet; technologies that are in school (such as PCs, laptops, tablets, webcams, whiteboards, digital video equipment, etc); and technologies owned by staff that are brought onto school premises (such as laptops, mobile phones, memory sticks etc).

The school's ICT systems and network cannot be regarded as private, and user accounts will be subject to random monitoring. They should be used primarily for school purposes, but occasional personal use is permitted. All ICT activities must conform to the norms of moral decency and not contravene ICT or other relevant legislation.

ICT Acceptable Use Policy Agreement for Staff

- I have read, understood and accept the ICT Acceptable Use Policy. I agree that all members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner.
- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I also understand that if I am found to have contravened any of these requirements that I may face disciplinary action.
- I accept that my use of the school IT facilities are monitored and the outcomes of the monitoring may be used.

Name:

Signed:

Date:

Appendix 2: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 3: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident