

Online Safety Policy

Approved: July 2026

Reviewed: July 2026

Next Review: Summer 2027

Contents

Aims	**1**
Legislation and guidance	2
Roles and responsibilities	2
Educating pupils about online safety	5
Educating carers/parents about online safety	6
Cyber-bullying	6
Acceptable use of the internet in school	8
EYFS Screentime Policy	8
The Use of AI	9
Pupils using mobile devices in school	9
Staff using work devices outside of school	10
How the school will respond to issue to misuse	10
Training	11
Monitoring arrangements	11
Links with other policies	13
APPENDIX 1: **ICT ACCEPTABLE USE AGREEMENT – PARENTS/CARERS**	14
APPENDIX 2: **ICT ACCEPTABLE USE AGREEMENT - STAFF, SUPPLY STAFF AND VISITORS**	

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' or 'mobile devices')
- 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

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
- Meeting digital and technology standards 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.

The policy also considers the National Curriculum computing programmes of study.

Roles and Responsibilities

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, briefing notes 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 those 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 governor who oversees online safety is R. McAvoy

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 (appendix 2)
- 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

The Headteacher

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

The Designated Safeguarding Staff & Computing Lead

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

The DSL and deputies take 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 and 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 contractor to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT contractor 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 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
- 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

This list is not intended to be exhaustive.

The ICT Contractor

The ICT 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 weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive. Our ICT contractor is a member of the AdEpt team who is supported by the computing lead.

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 2), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- 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 this immediately to the DLS or deputies
- Following the correct procedures by discussing with the DSL or deputies 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 onto 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
- 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.

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 (appendices 1 and 2)
- Ensure they have 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:

Parent Zone | At the heart of digital family life

Parents and carers | CEOP Education (thinkuknow.co.uk)

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 2).

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
- 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.

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 and twitter account. This policy will also be shared with parents/carers.

The school will let parents know what their children are being taught about online safety via the curriculum long term plans which are accessible on the school's website.

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.

Cyber-Bullying

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 the school anti-bullying policy).

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 classes.

Teaching staff 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 (see section 11 for more detail).

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.

Examining Electronic Devices

The headteacher, and any member of staff authorised to do so by the headteacher (refer to the school's behaviour policy), 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 or DSL lead.
- 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 headteacher or DSL lead 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 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, screening and confiscation

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

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 (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

We will monitor the websites visited by pupils, staff, volunteers, 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 appendices 1 to 3.

Alwoodley EYFS screen time policy

Taking on board the recent DfE screen use guidance, this policy outlines how our practice at Alwoodley takes this into consideration. Wherever possible, practical resources will be used in the place of screens.

Screen Use

Screens will be used in EYFS classrooms where it is deemed necessary to enhance the learning opportunity, have clear educational purpose and provide high-quality information, videos or graphics which cannot be replicated with hands on practical resources.

Children will **never be left to use screens independently**.

Adults will:

- watch alongside children
- discuss the content
- ask questions
- encourage predictions and thinking
- extend learning through conversation

Content shown on screens will be:

- Slow-paced
- To promote deeper thought and discussion
- Age appropriate
- Advert-free
- Checked beforehand
- Free from autoplay and scrolling features
- Limited to less than 1 hour each day

Screens will not be used for passive viewing or as a behaviour management tool.

SEND considerations

Screen-based assistive technology remains appropriate where it supports communication, inclusion, and access to learning.

The recommended screen-time limits do **not** apply to assistive technology used for SEND purposes.

AI
Children will not use AI tools or AI-enabled toys.

Pupils Using Mobile Devices in School

Pupils in key stage two may bring mobile devices into school, but are not permitted to use them during the school day. All mobile devices brought into school must be switched off and handed to a member of staff. This member of staff will place the mobile device into a locked cupboard. The mobile device will then be handed back to the pupil at the end of the day.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

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

Staff Using Work Devices Outside 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 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
- 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 2.

Work devices must be used solely for work activities.

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

The Use of AI

This policy outlines the principles and guidelines for the responsible use of Artificial Intelligence (AI) tools in our primary school. It aims to ensure that AI is used ethically, safely, and effectively to enhance the educational experience while protecting the rights and well-being of students and staff.

1. Scope of the Policy

This policy applies to all staff, and any other individuals who use AI tools within the school environment, including during classroom activities, homework, and school-related projects.

2. Guiding Principles

Educational Integrity: AI should be used to support learning and not replace the critical thinking and creativity that are essential in education.

Safety and Privacy: All AI tools must comply with data protection laws and ensure the confidentiality of student information.

3. Acceptable Use of AI Tools

Supportive Role: AI is a support tool for enhancing learning, not a replacement for human interaction or instruction. Staff are accountable for the content and quality of any work produced using AI.

Ethical Use: AI must be used in a fair and ethical manner, avoiding any form of discrimination or harm to individuals or groups based on characteristics such as age, gender, ethnicity, or disability.

4. Prohibited Uses of AI

In the Curriculum: Students must understand the difference between using AI as a tool and passing off AI-generated content as their own work.

Inappropriate Content: AI tools that generate harmful, misleading, or inappropriate content are not permitted in the school environment.

Data Misuse: Sharing personal or sensitive information with AI tools is prohibited. Users must be aware of the risks associated with data sharing and ensure compliance with relevant data protection legislation.

5. Implementation and Training

Education and Awareness: The school will provide training for staff on the ethical use of AI, including understanding its capabilities and limitations.

Monitoring and Review: The use of AI tools will be regularly monitored, and this policy will be reviewed annually to ensure it remains relevant and effective in addressing emerging challenges and opportunities in AI technology.

6. Conclusion

This policy is designed to foster a safe and productive learning environment where AI can be used responsibly to enhance educational outcomes. All members of the school community are expected to adhere to these guidelines to ensure the ethical and effective use of AI in our primary school.

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 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

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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

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, staff briefing and staff meetings).

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

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

Training will also help staff:

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

Monitoring Arrangements

The DSL will log behaviour and safeguarding issues related to online safety onto CPOMS

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

Links with Other Policies

Child protection and safeguarding policy

Behaviour policy

Staff code of conduct

Data protection policy and privacy notices

Complaints procedure

ICT and internet acceptable use policy

Appendix 1: ICT ACCEPTABLE USE AGREEMENT – PARENTS/CARERS



ICT ACCEPTABLE USE AGREEMENT – PARENTS/CARERS

Background and purpose

With access to rich dynamic content, connectivity across the globe, a platform for creativity and a place to engage in debate, digital technologies provide a powerful tool for learning. It is therefore essential that children are fully equipped to have the skills and knowledge to safely access and use digital technologies.

This **Parent/Carer Acceptable Use Agreement** is intended to help share the importance that the school places on keeping children safe with particular regard to online safety. It additionally intends to encourage parents/carers to be actively involved in their child's online safety education, including encouraging transparent behaviour, critical thinking and reporting.

The school will aim to provide every child with the best access it can to online technologies. Filtering, monitoring and alert systems will be in place to help protect children from unnecessary risks. The school will actively encourage children to think critically about content and communication from others and develop strategies for recognising inappropriate content/behaviours and how to deal with them. In return, the school expects the children to demonstrate that they are responsible users of digital technologies at all times.

Acceptable Use Agreement

By signing this agreement, you will have access to the school's systems and acknowledge that you agree to all the statements below.
Additionally, that you have read and understand school policies which have a bearing on this agreement.

- I will share good online behaviours with my child.
- I will emphasise the importance of the Acceptable Use Statements/School's rules my child has agreed to.
- I will understand the importance of accessing only age appropriate content and sites along with the pitfalls of social media.
- I will explain how to keep an appropriate digital footprint.
- I will discuss what is and isn't appropriate to share online.
- I will emphasise never to meet anyone online nor trust that everyone has good intentions.

- I will report any concerns I have whether home or school based.
- I will stress the importance of openness when being online and that no one should ever be too ashamed or embarrassed to tell a trusted adult if they have seen/shared anything concerning or have had inappropriate online contact.
- I will draw up an agreement of online safety rules for outside of school that are applicable even when my child is at a friend's home.
- I will avoid posting or replying to any comments about the school to social media that may have a negative impact. Any concerns or worries should be reported to the school in the first instance.

Permission Access
By signing below, you agree to allowing your child access to the school's internet and ICT systems. This also includes any educational subscription services. You are also aware that your child has signed/agreed to the school's Acceptable Use Agreement for pupils.

Parent/Carer Name: _____

Signature: _____

Date: _____

Child's Name: _____

Class: _____

**The school aims to comply with GDPR regulations at all times and as such follows strict protocol about how we use personal data and keep it safe, including the information on this form. It is important that you refer to the school's data protection policy or contact the school if you have any questions about data.*

Appendix 2: ICT ACCEPTABLE USE AGREEMENT - STAFF, SUPPLY STAFF AND VISITORS



ICT ACCEPTABLE USE AGREEMENT - STAFF, SUPPLY STAFF AND VISITORS

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with parents, pupils and others, they are asked to sign this code of conduct. Staff should consult the detail of the school's Policy for Staff Acceptable Use of ICT for further information and clarification.

- I appreciate that ICT includes a wide range of system, including mobile phones, personal digital assistants, cameras, email, internet and HCC intranet access and use of social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that it may be a criminal offence to use the school ICT system for a purpose not permitted.
- I understand that I am unable to communicate information which is confidential to the school or which I do not have the authority to share.
- I understand that school information systems and hardware may not be used for personal or private use without the permission of the Headteacher.
  I understand that my use of school information systems, internet and email may be monitored and recorded, subject to the safeguards outlined in the policy to ensure policy compliance.
- I understand the level of authority required to communicate with parents and pupils using the various methods of communication
- Only use internet enabled personal devices in line with this acceptable use policy and join the school's Wi-Fi.
- School site staff and leaders my use LCC mobile phones to complete duties (including taking photos of buildings & equipment) around the school and to be easily accessible – whilst using their LCC devices they must adhere to acceptable use policy.
- I understand that I must not use the school ICT system to access inappropriate content
- I understand that accessing, viewing, communicating and downloading material which is pornographic, offensive, defamatory, derogatory, harassing or bullying is inappropriate use of ICT
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone's account except my own.
- I will not install any software or hardware without permission.

- I will follow the school's policy in respect of downloading and uploading of information and material.
- I will ensure that personal data is stored securely and is used appropriately whether in school, taken off the school premises or accessed remotely. I will not routinely keep personal data on removable storage devices. Where personal data is required, it will be password protected/encrypted and removed after use.
- I will respect copyright, intellectual property and data protection rights.
- I understand use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- I will report any incidences of concern regarding children's safety to the Child Protection Liaison Officer or Headteacher.
- I will report any incidences of inappropriate use or abuse of ICT and inappropriate electronic communications, whether by pupils or colleagues, to the Headteacher, or if appropriate, the Chair of Governors.
- I will ensure that any electronic communication undertaken on behalf of the school, including email and instant messaging are compatible with my professional role and that messages do not present personal views or opinions and cannot be misunderstood or misinterpreted.
- I understand the school's stance on use of social networking and given my professional role working with children, will exercise care in any personal use of social networking sites.
- I will ensure that any electronic communications with pupils, where permitted, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote online-safety with pupils in my care and help them to develop a responsible attitude to system use, communication and publishing.
- I understand that inappropriate use of personal and other non-school based ICT facilities can have implications for my employment at the school where this becomes known and that activities undertaken are inconsistent with expectations of staff working with children.

The school may exercise its right to monitor the use of the school's ICT systems and accesses, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's ICT systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, images or sound.

I have read and understand the Policy for Staff Acceptable Use of ICT and understand that inappropriate use may be considered to be misconduct or gross misconduct and may, after proper investigation, lead to a disciplinary sanction or dismissal. I understand that if I need any clarification regarding my use of ICT facilities, I can seek such clarification from any member of the Senior Leadership Team.

Staff Name: _____

Signature: _____

Date: _____