Come as you are and leave as a champion

Online Safety Policy

Hempstalls Primary School

Approved by:	Governing Body	**Date:** 29th November 2023
Last reviewed on:	Autumn Term 2023	
Next review due by:	Autumn Term 2024	

Roles and Responsibilities

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Full Governors, which the Online Safety Governor will attend. This governor will liaise closely with the school Online Safety Coordinator each term, who will update the committee with regular information about online safety incidents and monitoring reports. The role of the Online Safety Governor includes:

- termly meetings with the Online Safety Leader
- termly monitoring of Online safety incident logs
- termly monitoring of filtering/change control logs
- reporting to relevant Governors committee at least annually

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any subcommittee/group involved in ICT/online safety/health and safety/child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association or other relevant organisation.
- Participation in school training / information sessions for staff or parents

Head Teacher and Senior Leader

The Head Teacher is responsible for ensuring the safety (including online safety) of members of the school community, as the designated Child Protection Coordinator, though the day to day responsibility for online safety will be delegated to the Online safety Leader.

The Head Teacher/Senior Leaders are responsible for ensuring that the Online safety Leader and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Head Teacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Senior Leadership Team will receive regular monitoring reports from the Online safety Leader.

The Head Teacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see SSCB website for a flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR/Disciplinary Procedures)

Online Safety Leader

- leads the online safety committee
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Academy trust
- Liaises with Entrust LST
- liaises with school ICT technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Online safety Governor to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meeting/committee of Governors
- reports regularly to Senior Leadership Team

Network Manager/Technical Staff:

Entrust Learning Technologies is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the online safety technical requirements outlined in the Staffordshire Security Policy and Acceptable Usage Policy and any relevant Local Authority Online safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- the school's filtering policy is applied and updated on a regular basis
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network/ remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online safety Leader /Head Teacher / Senior Leader for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Online safety Leader/Head Teacher / Senior Leader for investigation / action / sanction
- personal mobile phones must be stored in a locked cabinet during the school day and only used whilst children are not present. It is strongly recommended that staff passcode their mobile phone
- Under no circumstances should a member of staff take photographs or videos of pupils on their mobile phone or personal camera
- Any content on your mobile phone should not be shared with pupils
- digital communications with students / pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems

- staff should never give their e-mail address, personal telephone number, home address to pupils or their parents
- any telephone calls made top parents must be so using the school's office telephone. However, during school trips a school mobile telephone will be provide for this purpose.
- any text messages sent to parents must be sent via the school office
- online safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school online safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned student pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully
- understand the school online safety policy and Acceptable Use Policies

- The Online safety Leader will receive regular updates through attendance at Entrust training sessions and by reviewing guidance documents released by BECTA, the LEA and others.
- This Online safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online safety Leader will provide advice, guidance and training as required to individuals as required

Home/School Laptops

Each class teacher is provided with a laptop, unless the class teacher chooses to decline the offer. This laptop is for personal use only and it is the teachers responsibility to use it appropriately. Personal use is defined as being used or work purposes only and should not be used for personal activity such as online shopping. It is also a requirement that devices are not used by non-employees of the Trust e.g. a child or partner.

Designated person for Child Protection

should be trained in online safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Governors Committee

Members of the Governors committee and School Council will assist the Online safety Leader with:

- the review and monitoring of the school online safety policy / documents.
- the review and monitoring of the school filtering policy

Pupils

are responsible for:

- using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems (at KS1 parents are expected to sign on behalf of the pupils)
- each time a pupil logs on to a school computer they must agree to the Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online safety Policy covers their actions out of school, if related to their membership of the school.

The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.
Online safety education will be provided in the following ways:

- A planned online safety programme is provided as part of ICT, PSHEC and other lessons and is regularly revisited
- Key online safety messages will be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils are taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information
- Pupils are encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems and internet will be posted in all rooms
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Parents and Carers:

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will therefore take every opportunity to provide information and awareness to parents and carers through parents' evenings, newsletters, letters, website. Parents and carers will be responsible for:

- endorsing (by signature) the Student / Pupil Acceptable Use Policy
- accessing the school website on-line pupil records in accordance with the relevant school Acceptable Use Policy.

Community Users:

Community Users who access school ICT systems and VLE as part of the Extended School provision will be expected to sign a Community User AUP, before being provided with access to school systems.

Appendix 1

Internet Filtering and Monitoring Policy

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. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the online safety technical requirements outlined in the LA Security Policy and Acceptable Usage Policy and any relevant Local Authority Online safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling are securely located and physical access is restricted
- All users have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Online safety Leader.
- All users (at Year 1 and above) are provided with a username and password by the ICT Coordinator who will keep an up to date record of users and their usernames.
- The "administrator" password for the school ICT system, used by SLT (Staffordshire Learning Technologies) and the ICT Coordinator/Online safety Leader is available to the Head Teacher and is kept in a secure place.
- Users are responsible for the security of their username and password and must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by Entrust.
- In the event of the ICT Coordinator needing to switch off the filtering for any reason, or for any user, this will be logged.
- Any filtering issues will be reported immediately to SLT (Entrust Learning Technologies).
- Requests from staff for sites to be removed from the filtered list will be considered by the Head Teacher and ICT Coordinator/Online safety Leader. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Pupils and Personnel Committee.
- Teachers regularly monitor and record the activity of users on the school ICT systems. Users are made aware of this in the Acceptable Use Policy.
- A system is in place for users to report any actual / potential online safety incident to the ICT Coordinator/Online safety Leader, who will inform the Head Teacher, Governors and ELT (Entrust Learning Technologies).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system. Each visitor will be given a group login username and password. No documents will be saved in this area.
- Staff do not have permission rights to install programs on school workstations / portable devices. Requests can be made by staff to the ICT Coordinator who will contact SLT (Staffordshire Learning Technologies).
- The school infrastructure and individual workstations are protected by up to date virus software.(Symantec)
- Personal data will not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

- Filtering systems will be monitored by the Headteacher and chair of Governors and ICT technician

Appendix 2

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Verbal permission should be requested before taking digital or video images.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Names will not be used to identify pupils in photographs published on the website.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work will only be published with the permission of the pupil and parents or carers.

<u>Rules for Responsible Use of Digital/Video Images</u>

- I understand the risks associated with the taking, use, sharing, publication and distribution of images.
- I recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- I will request verbal permission before taking digital or video images.
- I will take care when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- I will always ask permission before I take, use, share, publish or distribute images of others.
- Names will **<u>not</u>** be used to identify pupils in photographs published on the website.
- I will only publish work with permission and label with only the first name.

Appendix 3

Use of Digital/Video Images Permission Form

Dear Parents

Digital/Video Images within School

The use of digital and video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons and displayed within school. We may also make video or webcam recording for school to school conferences, monitoring or educational use. Please read and discuss the rules overleaf with your child.

Permission Form

Images may also be used to celebrate success through their publication on the school website. We will always ensure that when images are published in this way the child's name is not used. Pieces of work may also be published on the school Learning Platform or website. We will always ensure that only the child's first name is used in these instances. Parents are requested to sign the permission form below to allow the school to take and use images of their child in this way and publish pieces of work by their child.

Occasionally we invite photographers from local newspapers or the Local Authority to promote school events in the public media. Under these circumstances we will contact you for further permission.

Photos taken by Parents/Carers for Personal Use
Please be aware that any digital or video images taken at school events, which include images of children other than your own, should only be for private retention and not published in any manner including personal websites.

Yours sincerely

Computing and Online Safety Coordinator

Appendix 4

Responding to incidents of misuse

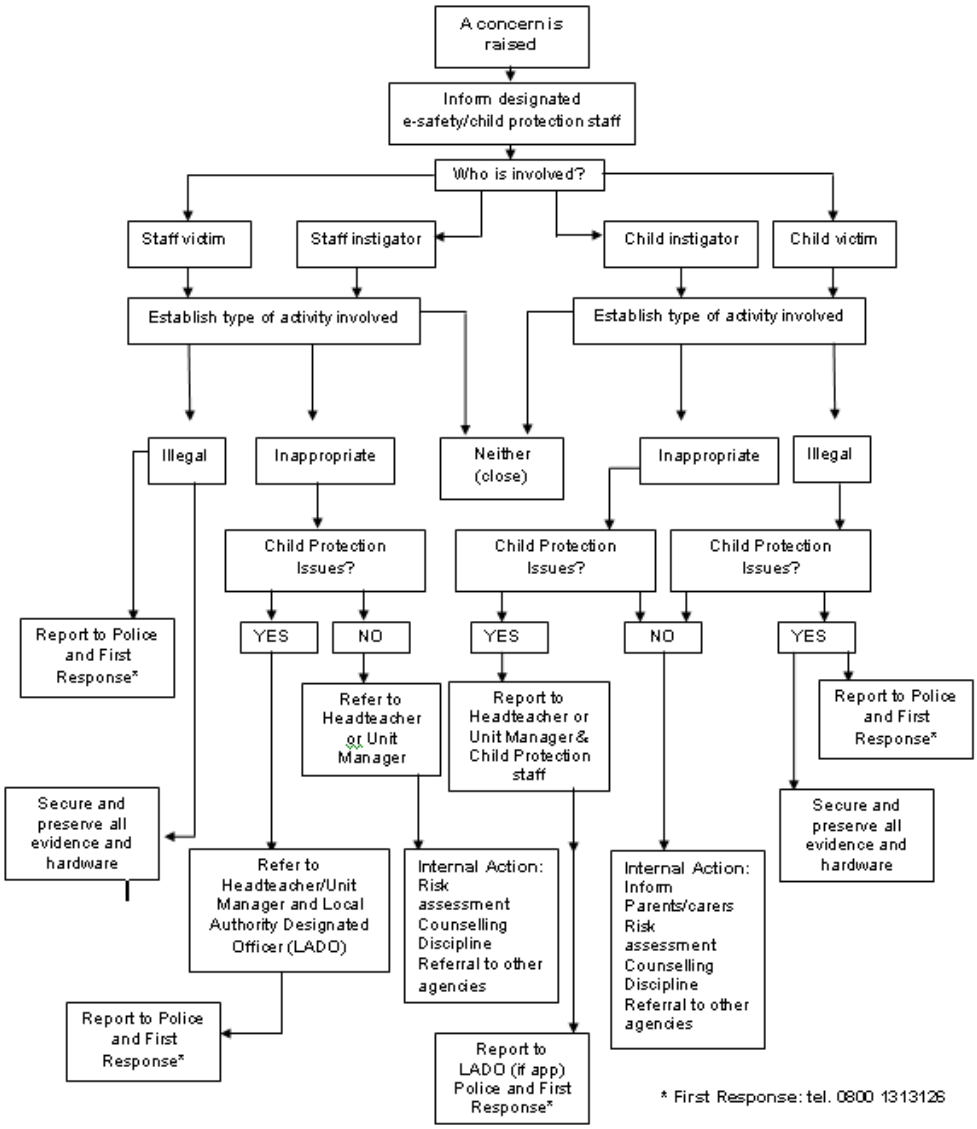
It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity E.g.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The flow chart from the Staffordshire Safeguarding Children's board– below and http://www.staffsscb.org.uk/online safetyToolkit/IncidentResponse/ should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

Staffordshire Local Safeguarding Children Board



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event then contact the **Staffordshire Safeguarding Children's Board.** It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with in line with our Acceptable Use, Behaviour and Friendship Policies.

Appendix 5

Acceptable Use Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that students pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

General use of computers

- The use of school computers will be permitted only for purposes directed by the school.
- Users are not permitted to access and amend another user's work without permission.
- All computers connected to the internet will be protected by anti-virus software which will be kept up to date.
- No files should be brought in from home and loaded on the school system without the permission of the ICT coordinator.
- The school reserves the right to look at any files on their systems.
- The school reserves the right to deny access to school computer systems.

Internet Access

- The school provides Internet access for educational purposes and should only be used for these purposes.
- Parents will be asked to sign a contract indicating that they understand the issues and give consent for their child to use the internet.

Use of email

- Any user of the school email system must not use the system to communicate inappropriate material.
- Email messages sent and received from school computers will be moderated by staff.

Publishing on the Internet

- Any images of children will **not be named.**
- Children's work will be labelled with their **first name only**.
- No personal information will revealed on the web or to other internet users.

Appendix 6

Rules for Responsible Use of ICT and the Internet

Rules for Responsible Use of ICT and the Internet

- I will treat school ICT equipment with care and respect.
- I will only use school computers for school work.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will ask permission from a member of staff before using the Internet.
- I will tell a member of staff if I find any unpleasant material on a site.
- I understand that school may check which sites I have visited.
- I will only email people I know or my teacher has approved.
- The messages I send will be polite and responsible.
- I will not give out my own details such as my name, phone number or home address.
- I will report any unpleasant material or messages sent to me.
- I know that my use of ICT can be checked and that my parent/carer will be contacted if a member of school staff is concerned about my online safety.

Appendix 7

AUP Poster

Enjoy using the Internet, but to make sure that you are safe online you must:

- ask permission from a member of staff before using the Internet.
- tell a member of staff if you find any unpleasant material on a site.
- understand that school may check which sites you have

Look after the ICT equipment … other children use it too!

- I will treat school ICT equipm with care and respect.
- I will only use computers for school work.
- I will not tell other people my ICT pass-

Everyone in the school should be allowed to use the Internet and email and you can make this happen if you:

- only email people you know or your teacher has approved.
- always use kind words when writing an email.
- report any unpleasant material or messages sent to you.

The Internet is for classwork not for playing games.

How to stay SAFE:
If you, by mistake, go on a website that you know is unsafe, let your teacher know straight away.
If you receive an email from someone that you find upsetting, let your teacher know straight away.
If you see anything that makes you feel worried, tell an adult you trust. You can talk to your mum, dad or teacher.

REMEMBER: ALL INTERNET ACCESS, including e-mail, IS MONITORED

Appendix 8

Rules for Responsible Use of ICT and the Internet – permission form

Dear Parents

Rules for Responsible Use of ICT and the Internet

ICT including the internet, learning platforms, e-mail and mobile technologies have become an important part of learning in our school. We expect all pupils to be safe and responsible when using any ICT. It is essential that pupils are aware of the 'Rules for Responsible Use of the Internet' and know how to stay safe when using any ICT. You may be interested to know that we don't use social networking sites such as 'Facebook' in school as the minimum age for use is 13.

Please read and discuss the rules overleaf with your child and return the permission form below.

Yours sincerely

ICT Coordinator

Hempstalls Primary School

Rules for Responsible Use of ICT and the Internet – Permission Form

I grant permission for my child to have access to use the Internet and I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access e-mail, employing appropriate teaching practice and teaching online safety skills to pupils. I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies.

I understand that the school can check my child's computer files, and the Internet sites they visit, and that if they have concerns about their online safety or e-behaviour that they will contact me.

I have discussed the Rules for Responsible Use of the Internet and my child agrees to follow them and to support the safe use of ICT at Westfield Community Primary School.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's online safety.

Name of Child:

Class:

Signed:
(Parent/Carer)

Rules for Responsible Use of ICT and the Internet

- I will treat school ICT equipment with care and respect.
- I will only use school computers for school work.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will ask permission from a member of staff before using the Internet.
- I will tell a member of staff if I find any unpleasant material on a site.
- I understand that school may check which sites I have visited.
- I will only email people I know or my teacher has approved.
- The messages I send will be polite and responsible.
- I will not give out my own details such as my name, phone number or home address.
- I will report any unpleasant material or messages sent to me.
- I know that my use of ICT can be checked and that my parent/carer will be contacted if a member of school staff is concerned about my e- safety.