# Policy Name

E-safety Policy

Approved: September 2023

Approved by: Management Board

Next Review: September 2024

# Table of Contents

## Safety Ethos

### Aims and Policy Scope

Heathcote School believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.

Heathcote School identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.

Heathcote School has a duty to provide the community with quality Internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions.

Heathcote School identifies that there is a clear duty to ensure that all children and staff are protected from potential harm online.

The purpose of Heathcote School's online safety policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that Heathcote School is a safe and secure environment.
- Safeguard and protect all members of the School community online.
- Raise awareness with all members of the School community regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

This policy applies to all staff including the directors, teachers, support staff, external contractors , visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.

This policy applies to all access to the internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.

This policy must be read in conjunction with other relevant school policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour, ICT Policy, Acceptable Use Policies, confidentiality and relevant curriculum policies including computing, Personal Social and Health Education (PSHRE), Citizenship and Relationships and Sex Education (CRSE). This policy also adheres to the principles set out in KCSIE (2022).

## Key Contacts/DSLs

| | |
|---|---|
| DSL Nadine Solsberg, Bursar+ Director for Safeguarding | n.solsberg@heathcoteschool.co.uk |
| Deputy DSL (EYFS): Samantha Scott, Headteacher | s.scott@heathcoteschool.co.uk |
| Deputy DSL Georgina Pennycook, Teacher | g.pennycook@heathcoteschool.co.uk |
| Deputy DSL Kelly Collins, Nursery Manager | k.collins@heathcoteschool.co.uk |
| Head of ICT/Online Safety: Liam Daniels | l.daniels@heathcoteschool.co.uk |
| Filtering and Monitoring, Director; Nadine Solsberg | n.solsberg@heathcoteschool.co.uk |

***See Appendix B for detailed contact list**

## Key Responsibilities for the Community

### The key responsibilities of the school management and leadership team are:

- Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school community.
- Ensuring that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture.
- Supporting the Designated Safeguarding Lead (DSL) by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including an Acceptable Use Policy which covers appropriate professional conduct and use of technology.
- To ensure that robust and appropriate systems for filtering and monitoring usage are in place to protect children from inappropriate content which meet the needs of the school community whilst ensuring children have access to required educational material.
- To work with and support technical staff in monitoring the safety and security of school systems and networks and to ensure that the school network system is actively monitored.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is embedded within a progressive whole school curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- To be aware of any online safety incidents and ensure that external agencies and support are liaised with as appropriate.
- Receiving and regularly reviewing online safeguarding records and using them to inform and shape future practice.
- Ensuring there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- To ensure a member of the Board is identified with a lead responsibility for supporting online safety. (Mrs Nadine Solsberg)
- Auditing and evaluating current online safety practice to identify strengths and areas

for improvement.

- To ensure that the Designated Safeguarding Lead (DSL) works with the online safety lead.

## The key responsibilities of the Designated Safeguarding Lead are:

- Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends regarding online safety.
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Work with the school lead for data protection and data security to ensure that practice is in line with current legislation.
- Maintaining a record of online safety concerns/incidents and actions taken as part of the schools safeguarding recording structures and mechanisms.
- Monitor the schools online safety incidents to identify gaps/trends and use this data to update the schools education response to reflect need
- To report to the school management team, board and other agencies as appropriate, on online safety concerns and local data/figures.
- Liaising with the local authority and other local and national bodies, as appropriate.
- Working with the school leadership and management to review and update the online safety policies, Acceptable Use Policies (AUPs) and other related policies on a regular basis (at least annually) with stakeholder input.
- Ensuring that online safety is integrated with other appropriate school policies and procedures.
- Meet regularly with the board member with a lead responsibility for CP including online safety.

## The key responsibilities for all members of staff are:

- Contributing to the development of online safety policies.
- Reading the school Acceptable Use Policies (AUPs) and adhering to them.
- Taking responsibility for the security of school systems and data.

- Having an awareness of a range of different online safety issues and how they may relate to the children in their care.
- Modelling good practice when using new and emerging technologies.
- Embedding online safety education in curriculum delivery, wherever possible.
- Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures.
- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Demonstrating an emphasis on positive learning opportunities in all areas of ICT.
- Taking personal responsibility for professional development in this area.

**In addition to the above, the key responsibilities for staff managing the technical environment (Mr Liam Daniels – online safety lead) and areas outsourced to IT4Offices (it4) our agreed IT support are:**

- Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the schools filtering policy is applied as set up by IT4 (see appendix) and updated on a regular basis and that responsibility for its implementation is shared with the DSL.
- Ensuring that the use of the school's network is regularly monitored and reporting any deliberate or accidental misuse to the DSL.
- Report any breaches or concerns to the DSL and leadership team and together ensure that they are recorded and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Report any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.

- Providing technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensure that, if relevant, appropriately strong passwords are applied and enforced for all but the youngest users.

**The key responsibilities of children and young people are:**

- Contributing to the development of online safety policies.
- Reading the school Acceptable Use Policies (AUPs) and adhering to them.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong and supporting others that may be experiencing online safety issues.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

## The key responsibilities of parents and carers are:

- Reading the school Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of technology and social media.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.

- Using school systems, such as learning platforms, and other network resources, safely and appropriately where this is appropriate.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

# Online Communication and Safer Use of Technology

## Managing the school website

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE).
- The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The head of marketing will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate in all marketing material.
- The website will comply with the school's guidelines for publications including accessibility respect for intellectual property rights, privacy policies and copyright.
- The administrator account for the school website will be safeguarded with an appropriately strong password and only known to Directors and administrators.
- The school will post information about safeguarding, including online safety, on the school website for members of the community.

## Publishing images and videos online

- Images will be shared online only via approved channels and only with explicit parental consent.
- Prior to entry to the school, consent is requested for the appropriate use of children's images in line with Data Protection Act 2018.

## Managing email

- All members of staff are provided with a specific school email address to use for internal communication and any official communication ie to organise school trips
- All parent communication should be via the school office and any emails received should be forwarded to the office and responded to by the office.
- The use of personal email addresses by staff for any official school business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Access to school email systems will always take place in accordance to data protection legislation and in line with other appropriate school policies.
- Members of the community must immediately tell a designated member of staff if they

receive offensive communication and this will be recorded in the school safeguarding records.

- Staff will be encouraged to develop an appropriate work life balance when responding to email, especially if communication – this is particularly pertinent where staff received email directly to personal mobile devices or home PCs.
- When accessing emails outside of the setting, particular care must be given to confidentiality and data protection.
- Email sent to external organisations should be written carefully before sending, in the same way as a letter written on school headed paper would be.
- If the communication is of a sensitive nature, a member of SLT should be copied in and consulted before sending.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

## Official software used for delivering remote learning provision

- The school uses Microsoft Teams as the default product for delivery of remote learning and internal communication.
- Staff will ensure that remote learning opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access events are appropriately safe and secure.

### Users

- Remote learning will be supervised appropriately for the pupils' age and ability and a teacher/adult will always be present.
- Remote learning will take place via official and approved communication channels following a robust risk assessment.

### Content

- If third party materials are to be included, the school will check that recording is acceptable to avoid infringing the third party's intellectual property rights.
- The school will establish dialogue with other conference participants before taking part in a
- remote learning session. If it is a non-school site, the school will check that they are delivering material that is appropriate for the class.

## Accessing the School's MIS Hub

Staff should access the Hub via school devices to ensure that access to the sensitive information is kept secure. If there is a need to access information and a member of staff does not have access to a school device, permission MUST be sought from the Headteacher or Bursar.

In this instance extreme care should be taken to log out of the portal completely and the history wiped.

## Appropriate and safe classroom use of the internet and any associated devices

- Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum. Please access specific curriculum policies for further information.
- The school's internet access will be designed to enhance and extend education.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- Supervision of pupils will be appropriate to their age and ability:
  - At Early Years Foundation Stage and Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials which supports the learning outcomes planned for the pupils' age and ability.
  - At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. Children will be directed to online material and resources, which support the learning outcomes planned for the pupils' age and ability.
- All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place.
- All ipads will be stored securely out of sight.
- Members of staff will always evaluate websites, tools, video and apps fully before use in the classroom or recommending for use at home.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will use age appropriate applications on interactive whiteboards and search tools and websites designed for child use.
- The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject and will

be viewed as a whole-school requirement across the curriculum.

- The school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment through online learning portals or LPs (e.g. Teams) in an age appropriate manner. Teachers will monitor all chats or content posted by children in such environments; see below:

## Management of school learning platforms/portals/gateways e.g. Teams

- Where a class teacher uses such an environment, SLT must be aware and will regularly monitor the usage of the Learning Platform (LP) in all areas, in particular message and communication tools and publishing facilities.
- Pupils will be advised about acceptable conduct and use when using the LP.
- Only members of the current pupil, parent/carers and staff community will have access to the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- When staff, pupils' etc. leave the school, their account or rights to specific school areas will be disabled.
- Any concerns about content on the LP will be recorded and dealt with in the following ways:
  - The material will be removed by the site administrator
  - Access to the LP for the user may be suspended.
  - A pupil's parent/carer may be informed.

# Social Media Policy

## General social media use

- Expectations regarding safe and responsible use of social media will apply to all members of the Heathcote School community and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking sites, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.
- All members of the School community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the School community.
- The school may control pupil and staff access to social media and social networking sites whilst on site and when using school provided devices and systems
- The use of social networking applications during school hours for staff personal use is permitted using personal devices only during breaks.
- Inappropriate or excessive use of social media during school/work hours or whilst using school devices may result in disciplinary or legal action and/or removal of Internet facilities.
- Any concerns regarding the online conduct of any member of the School community on social media sites should be reported to the leadership team and will be managed in accordance with policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.
- Any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with relevant policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

## Official use of social media

- Heathcote School's official social media channels are:
  - *Twitter (@Heathcoteschoo1), Facebook (Heathcote School), Instagram (Heathcoteschooldanbury)*

Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.

- Official use of social media sites as communication tools will be risk assessed and formally approved by the Directors.
- Official school social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes.
- Staff will use school provided email addresses to register for and manage any official approved social media channels.
- Members of staff running official social media channels will sign a specific Acceptable Use Policy (AUP) to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official social media sites will comply with legal requirements including GDPR, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
- Official social media use will be in line with existing policies including anti-bullying and child protection.
- Images or videos of children will only be shared on official social media sites/channels in accordance with the image use policy.
- Information about safe and responsible use of social media channels will be communicated clearly and regularly to all members of the community.
- Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the school website and take place with written approval from the Leadership Team.
- Leadership staff must be aware of account information and relevant details for social media channels in case of emergency, such as staff absence.
- Parents/Carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

## Staff personal use of social media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and

communicated via regular staff training opportunities.

- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Acceptable Use Policy.

- All members of staff are advised not to communicate with or add as 'friends' any current or past children/pupils or current or pupils' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the head teacher and it is the responsibility of the staff member to notify their line manager.

- All communication between staff and members of the school community on school business will take place via official approved communication channels (*such as an official setting provided email address or phone numbers*)

- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted. Any existing relationships of this type must be disclosed to line managers.

- Any communication from pupils/parents received on personal social media accounts will be reported to the schools designated safeguarding lead.

- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites.

- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.

- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with schools policies (safeguarding, confidentiality, data protection etc.) and the wider professional and legal framework.

- Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.

- Members of staff will notify the SLT immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school.

- Members of staff will ensure that they do not represent their personal views as that of the school on social media and will never portray the school in a negative light and never discuss or post concerning individual children or their families whether explicitly named or merely alluded to.

- School email addresses will not be used for setting up personal social media accounts.
- Members of staff who follow/like the school social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

## Staff official use of social media

- If members of staff are participating in online activity as part of their capacity as an employee of the school, then they are requested to be professional at all times and to be aware that they are an ambassador for the school.
- Staff using social media officially will disclose their official role/position but always make it clear that they do not necessarily speak on behalf of the school.
- Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Staff using social media officially will always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Staff must ensure that any image posted on any official social media channel have appropriate written parental consent.
- Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
- Staff using social media officially will inform their line manager, the Designated Safeguarding Lead of any concerns such as criticism or inappropriate content posted online.
- Staff will not engage with any direct or private messaging with children or parents/carers through social media and will communicate via official communication channels.
- Staff using social media officially will sign the school social media Acceptable Use Policy.

## Pupils use of social media

- Safe and responsible use of social media sites will be outlined for children and their parents as part of the Acceptable Use Policy.
- Personal publishing on social media sites will be taught to pupils as part of an embedded and progressive education approach via age appropriate sites, which have been risk, assessed and approved as suitable for educational purposes.
- Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites, which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.

- Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Parents will be informed of any official social media use with pupils and written parental consent will be obtained, as required.
- Any official social media activity involving pupils will be moderated by the school where possible.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school would consider it inappropriate to encourage or allow use of such sites in school for any child, whilst acknowledging that many children will have such accounts outside of the school.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents/carers, particularly when concerning any underage use of social media sites.

# Use of Personal Devices and Mobile Phones

## Rationale regarding personal devices and mobile phones

- The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members of the Heathcote School community to take steps to ensure that mobile phones and personal devices are used responsibly.
- The use of mobile phones and other personal devices by young people and adults will be decided by the school and is covered in appropriate policies including the school Acceptable Use or Mobile Phone Policy and is at the Head's discretion, where children may, for example, be permitted to bring personal devices on residential trips.
- The School recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff and parents/carers but requires that such technologies need to be used safely and appropriately within schools.

## Expectations for safe use of personal devices and mobile phones

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies, such as safeguarding and communication.
- Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms, toilets and swimming pools.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the discipline/behaviour policy.
- Members of staff will have access to a landline and email address for the contact of parents.
- All members of the School community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.
- All members of the School community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.
- All members of the School community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the schools policies.
- School mobile phones and devices must always be used in accordance with the Acceptable Use Policy and any other relevant policies.
- School mobile phones and devices used for communication with parents and pupils must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.

## Pupils use of personal devices and mobile phones

**The following statements recognise that our children are not of the age to generally bring mobile devices into school and never without permission and as a general rule children are not allowed to have mobile phones in school or on school trips; this is inline with the School's Use of Mobile Phone Policy, however;**

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- Pupil's personal mobile phones and personal devices will be kept securely in the office, switched off and kept out of sight.
- Mobile phones or personal devices will not be used by pupils during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff in a BYOD (Bring your own device activity).
- If members of staff have an educational reason to allow children to use their mobile phones or personal devices as part of an educational activity then it will only take place when approved by the Leadership Team. Examples may include a child sharing a presentation with the class on an iPad.
- If a pupil needs to contact his/her parents/carers they should speak to the school secretary.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members.
- Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the schools behaviour or bullying policy or could contain youth produced sexual imagery (sexting). The phone or device may be searched by a member of the Leadership team with the consent of the pupil or parent/carer.
- Searches of mobile phone or personal devices will only be carried out in accordance with the schools policy. (Appropriate for schools only and must link to appropriate policy. See https://www.gov.uk/government/publications/searching-screening-and-confiscation)
- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal the DSL will take further action as required.

## Staff use of personal devices and mobile phones

- Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with leaders/managers.
- Teachers will use photographic evidence to record activities and milestones in the children's education. This photographic evidence may be used in school displays, newsletter and on the school website or in publicity items and newspapers. Parents sign a consent form giving permission for children to be photographed when they join the school.

- Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.
- Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law e.g. data protection as well as relevant school policy and procedures e.g. confidentiality, data security, Acceptable Use.
- Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.
- Personal mobile devices should be used with great care as a resource within the classroom (e.g. as a calculator or torch) and alternatives should be sought.
- Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches the school policy, then disciplinary action will be taken.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, then the police will be contacted.
- Any allegations against members of staff involving personal use of mobile phone or devices will be responded to as outlined in the staff handbook.

## Visitors use of personal devices and mobile phones

- Parents/carers and visitors must use mobile phones and personal devices in accordance with the schools acceptable use policy.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

## EYFS

The EYFS does not allow the use of mobile phones, any image recording device, or personal technical equipment such as laptops, ipads etc to be used in the setting without prior permission of the Head of EYFS.

### Procedures

- We do not allow the use of mobile phones, on the premises either indoors or in the outdoor play area in the EYFS.
- Staff are asked to keep their mobile phones with their personal belongings while children are on the premises, they may of course use their phones during their lunch break in the school staff room or away from the EYFS classrooms.
- In case of emergency, staff are advised that they may give the School phone number 01245 223131 to immediate family and schools etc to be contacted on.
- Parents and visitors will be asked to ensure their phones are kept in their bags for the duration of their visit.
- If parents or visitors need to use their mobile phone they will be asked to go to a safe place in order to do so.

### Cameras and videos

- Members of staff must not bring their own cameras or video recorders into the setting
- Photographs and recordings of children are only taken on equipment belonging to the setting
- Camera and video use is monitored by the Headteacher

### Mobile Phones

Mobile phones must not used at any time within the EYFS setting for photography or otherwise. The exception to this rule would be in a case of emergency when staff needed to contact the office urgently – ie lockdown procedures. Apart from this all mobile phones should be kept with personal belongings.

## Policy Decisions

### Reducing online risks

- Heathcote School is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.
- Emerging technologies will be examined for educational benefit and the school leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed.
- The school will ensure that appropriate filtering and monitoring systems are in place to prevent staff and pupils from accessing unsuitable or illegal content such as firewalls and network monitoring.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not always possible to guarantee that access to unsuitable material will never occur via a school computer or device and children should know how to respond (don't panic, tell a teacher if this happens).
- The school will audit technology use to establish if the online safety (e–Safety) policy is adequate and that the implementation of the policy is appropriate.
- Methods to identify, assess and minimise online risks will be reviewed regularly by the schools leadership team.

# Engagement Approaches

## Engagement and education of children and young people

- An online safety (e-Safety) curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils.
- Education about safe and responsible use will precede internet access.
- Pupils input will be sought when writing and developing school online safety policies and practices, including curriculum development and implementation.
- Pupils will be supported in reading and understanding the Acceptable Use Policy in a way which suits their age and ability.
- All users will be informed that network and Internet use will be monitored.
- Online safety (e-Safety) will be included in the PSHRE, RSE, Citizenship and Computing programmes of study, covering both safe school and home use.
- Online safety (e-Safety) education and training will be included as part of the transition programme across the Key Stages and when moving between establishments.
- Acceptable Use expectations and Posters will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.
- External support will be used to complement and support the schools internal online safety (e-Safety) education approaches.
- The school will reward positive use of technology by pupils.
- The school will implement peer education to develop online safety as appropriate to the needs of the pupils.

## Engagement and education of children & young people considered to be vulnerable

- Heathcote School is aware that some children may be considered to be more vulnerable online due to a range of factors.
- Heathcote School will ensure that differentiated and ability appropriate online safety (e-Safety) education is given, with input from specialist staff as appropriate (e.g. SENCO).

### Engagement and education of staff

- The online safety (e-Safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of our safeguarding responsibilities.
- Staff will be made aware that our Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential when using school systems and devices.

- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff in a variety of ways, on a regular (at least annual) basis.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- The school will highlight useful online tools which staff should use according to the age and ability of the pupils.

## Engagement and education of parents and carers

- Heathcote School recognise that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
- Parents' attention will be drawn to the school online safety (e-Safety) policy and expectations in newsletters, letters, school prospectus and on the school website.
- A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g. parent evenings, transition events, fetes and sports days.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Information and guidance for parents on online safety will be made available to parents in a variety of formats.
- Parents will be encouraged to role model positive behaviour for their children online.

# Managing Information Systems

## Managing personal data online

- Personal data will be recorded, processed, transferred and made available according to GDPR.
- Full information regarding the schools' approach to data protection and information governance can be found in the Schools Privacy Notice.

## Security and Management of Information Systems

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.
- Portable media may not be used without specific permission followed by an anti-virus /malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The computing coordinator/network manager will review system capacity regularly.
- All users will be expected to log off or lock their screens/devices if systems are unattended.

## Password policy

- All users will be informed not to share passwords or information with others and not to login as another user at any time.
- Staff must always keep their password private and must not share it with others or leave it where others can find it.
- All members of staff will have their own unique username and private passwords to access school systems such as email. Members of staff are responsible for keeping their password private.
- We require staff to use STRONG passwords for access into our system. Staff will be prompted to renew their password every 45 days.
- The system will automatically prompt a password change every 45 days.

## Filtering and Monitoring

- The Directors/IT Services provider will ensure that the school has age and ability appropriate filtering and monitoring in place whilst using school devices and systems to limit children's exposure to online risks.

- Mrs Solsberg is responsible for overseeing this operation, checks the reports and carries out filtering checks. She liases with our IT supplier to ensure they are aware of the most recent legislation.

- Mrs Solsberg ensures that all staff are sufficiently trained in Online Safety and that the IT Coordinator has completed e-safety training
- The school's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.
- All monitoring of school owned/provided systems will take place to safeguard members of the community.
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- The school uses filtered secure broadband connectivity which is appropriate to the age and requirement of our pupils.
- The school uses AVAST filtering system which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.
- If staff or pupils discover unsuitable sites, the URL will be reported to the IT Co-ordinator and will then be recorded and escalated to the DSL
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team and DSL
- All changes to the school filtering policy will be logged and recorded.
- Mr Daniels (Online Safety Lead) will carry out regular checks to ensure that the filtering methods are effective and appropriate
- Mrs Solsberg (DSL/Director) will monitor the checks that are made to ensure that the filtering methods selected are effective and appropriate.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Essex Police or CEOP immediately.

## Management of applications (apps) used to record children's progress

- The Headteacher is ultimately responsible for the security of any data or images held of children.
- Apps/systems which store personal data will be risk assessed prior to use such as WCBS/HUBmis
- Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs e.g. Tapestry in EYFS. Personal staff mobile phones or devices should not be used to access or upload content to any apps which record and store children's personal details, attainment or images.
- Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.
- Users will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.
- Parents will be informed of the schools expectations regarding safe and appropriate use (e.g. not sharing passwords or sharing images) prior to being given access.

## Responding to Online Incidents and Safeguarding Concerns

- All members of the community will be made aware of the range of online risks that are likely to be encountered including sexting, upskirting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils.
- All members of the school community will be informed about the procedure for reporting online safety (e-Safety) concerns, such as breaches of filtering, sexting, cyberbullying, illegal content etc.
- The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Essex Safeguarding Children Board thresholds and procedures.
- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Complaints about online/cyber bullying will be dealt with under the School's anti-bullying policy and procedure
- Any complaint about staff misuse will be referred to the head teacher
- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Pupils, parents and staff will be informed of the school's complaints procedure.
- Staff will be informed of the complaints and whistle blowing procedure.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- The school will manage online safety (e-Safety) incidents in accordance with the school discipline/behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Education Safeguards Team or Essex Police via 101 or 999 if there is immediate danger or risk of harm.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.
- If an incident of concern needs to be passed beyond the school community, then the concern will be escalated to the Education Safeguarding Team to communicate to other schools/settings locally.
- Parents and children will need to work in partnership with the school to resolve issues.

# Appendix A

## Procedures for Responding to Specific Online Incidents or Concerns

### Responding to concerns regarding Youth Produced Sexual Imagery or "Sexting"

- Heathcote School ensures that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating youth produced sexual imagery (known as "sexting").
- The school will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers via both internal RSE and PSHE and through the use of external providers.
- Heathcote School views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The school will follow the guidance as set out in the non-statutory UKCCIS advice 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB "Responding to youth produced sexual imagery" guidance
- If the school are made aware of incident involving creating youth produced sexual imagery, the school will:
- Act in accordance with the schools child protection and safeguarding policy and the relevant Essex Safeguarding Child Boards procedures.
- Immediately notify the designated safeguarding lead.
- Store the device securely.
- Carry out a risk assessment in relation to the children(s) involved.
- Consider the vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies)
- Make a referral to children's social care and/or the police (as needed/appropriate).
- Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Implement appropriate sanctions in accordance with the schools behaviour policy but taking care not to further traumatise victims where possible.
- Review the handling of any incidents to ensure that the school is implementing best practice and the leadership team will review and update any management procedures where necessary.
- Inform parents/carers about the incident and how it is being managed.
- The school will not view an images suspected of being youth produced sexual imagery unless there is no other possible option or there is a clear need or reason to do so (in these cases the image will only be viewed by the Designated Safeguarding Lead).
- The school will not send, share or save content suspected to be an indecent image of children and will not allow or request children to do so.

- If an indecent image has been taken or shared on the school's network or devices, then the school will take action to block access to all users and isolate the image.
- The school will take action regarding creating youth produced sexual imagery, regardless of the use of school equipment or personal equipment, both on and off the premises.
- The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

## Responding to concerns regarding Online Child Sexual Abuse & Exploitation

***Possible statements:***

- Heathcote School will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- Heathcote School views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Essex Police.
- If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), then it will be passed through to the CSET team by the DSL.
- If the school are made aware of incident involving online child sexual abuse of a child, then the school will:
  - Act in accordance with the school's child protection and safeguarding policy and the relevant Essex Safeguarding Child Boards procedures.
  - Immediately notify the designated safeguarding lead.
  - Store any devices involved securely.
  - Immediately inform Essex police via 101 (using 999 if a child is at immediate risk)
  - Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse e.g. using the Click CEOP report form: www.ceop.police.uk/safety-centre/
  - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
  - Make a referral to children's social care (if needed/appropriate).
  - Put the necessary safeguards in place for pupil(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
  - Inform parents/carers about the incident and how it is being managed.
  - Review the handling of any incidents to ensure that the school is implementing best practice and the school leadership team will review and update any management procedures where

necessary.

- The school will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.
- The school will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
- If pupils at other schools are believed to have been targeted then the school will seek support from the Education Safeguarding Team to enable other schools to take appropriate action to safeguarding their community.

## Responding to concerns regarding Indecent Images of Children (IIOC)

- Heathcote School will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.
- The school will take action regarding of Indecent Images of Children (IIOC) regardless of the use of school equipment or personal equipment, both on and off the premises.
- The school will take action to prevent access accidental access to of Indecent Images of Children (IIOC) for example using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.
- If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Essex Police.
- If the school is made aware of Indecent Images of Children (IIOC) then the school will:
  - Act in accordance with the school's child protection and safeguarding policy and the relevant Essex Safeguarding Child Boards procedures.
  - Immediately notify the school Designated Safeguard Lead.
  - Store any devices involved securely.
  - Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF), Essex police via 101 (using 999 if a child is at immediate risk) and/or the LADO (if there is an allegation against a member of staff).
- If the school are made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet then the school will:
  - Ensure that the Designated Safeguard Lead is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
- If the school is made aware that indecent images of children have been found on the schools' electronic devices then the school will:
  - Ensure that the Designated Safeguard Lead is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.

- Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.

- If the school is made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:
  - Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the school whistleblowing procedure.
  - Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
  - Follow the appropriate school policies regarding conduct.

## Responding to concerns regarding radicalisation and extremism online

***Possible statements:***

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils. This monitoring will be undertaken by our designated IT service provider, IT4Offices.
- When concerns are noted by staff that a child may be at risk of radicalisation online, then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the safeguarding policy.
- All staff have been trained in line with the prevent duty.
- Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including anti-bullying, behaviour etc. If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately via the Education Safeguarding Team and/or Essex Police.

## Responding to concerns regarding cyberbullying

***Possible Statements:***

- Cyberbullying, along with all other forms of bullying, of any member of Heathcote School community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.
- All incidents of online bullying reported will be recorded.
- There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Essex Police.

- Pupils, staff and parents/carers will be advised to keep a record of cyberbullying as evidence.
- The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the schools e-Safety ethos.
  - Sanctions for those involved in online or cyberbullying may include:
  - Those involved will be asked to remove any material deemed to be inappropriate or offensive.
  - A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
  - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
  - Parent/carers of pupils involved in online bullying will be informed.
  - The Police will be contacted if a criminal offence is suspected.

## Responding to concerns regarding online hate

- Online hate at Heathcote School will not be tolerated. Further details are set out in the school policies regarding anti-bullying and behaviour, available on the School's website.
- All incidents of online hate reported to the school will be recorded.
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures e.g. anti-bullying, behaviour etc. taking into account the age and understanding of the child(ren) involved.
- The Police will be contacted if a criminal offence is suspected. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Essex Police.

# Appendix B

## Online Safety (e-Safety) Contacts and References

### Essex Support and Guidance

**Essex County Councils Education Safeguards Team**:

https://schools-secure.essex.gov.uk/pupils/Safeguarding/Pages/Safeguarding.aspx

**Essex Online Safety Support for Education Settings**

| | |
|---|---|
| Service Area: | Safeguarding |
| Telephone: | 033301 31078 |
| Email: | jo.barclay@essex.gov.uk |

**Essex Police:** www.essex.police.uk

Contact Essex Police via 101

**Essex Safeguarding Children Board (ESCB):** http://www.escb.co.uk/

**Kent e–Safety Blog**: www.kentesafety.wordpress.com

## National Links and Resources

**Action Fraud:** www.actionfraud.police.uk

**BBC WebWise:** www.bbc.co.uk/webwise

**CEOP(Child Exploitation and Online Protection Centre):** www.ceop.police.uk

**ChildLine:** www.childline.org.uk

**Childnet:** www.childnet.com

**Get Safe Online:** www.getsafeonline.org

**Internet Matters:** www.internetmatters.org

**Internet Watch Foundation (IWF):** www.iwf.org.uk

**Lucy Faithfull Foundation:** www.lucyfaithfull.org

**Know the Net:** www.knowthenet.org.uk

| | |
|---|---|
| **Net Aware:** | www.net-aware.org.uk |
| **NSPCC:** | www.nspcc.org.uk/onlinesafety |
| **Parent Port:** | www.parentport.org.uk |
| **Professional Online Safety Helpline:** | www.saferinternet.org.uk/about/helpline |
| **The Marie Collins Foundation:** | http://www.mariecollinsfoundation.org.uk/ |
| **Think U Know**: | www.thinkuknow.co.uk |
| **Virtual Global Taskforce**: | www.virtualglobaltaskforce.com |
| **UK Safer Internet Centre:** | www.saferinternet.org.uk |
| **360 Safe Self-Review tool for schools:** | https://360safe.org.uk/ |
| **Online Compass (Self review tool for other settings):** | http://www.onlinecompass.org.uk/ |
| **Filtering and Monitoring** | www.testfiltering.com |

# Appendix C

## AUP for Staff using Social Media

### Staff Social Networking Acceptable Use Policy

*For use with staff running official school social media accounts*

1. As part of the school's drive to encourage safe and appropriate behaviour in the use of today's technology, I will support the school's approach to Online safety (e-Safety) . I am aware that the School Website, Facebook and/or Twitter are public and global communication tools and that any content posted may reflect on the school, its reputation and services. I will not use the site/page/group to express any personal opinions or create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring the school into disrepute.

2. I will not disclose information, make commitments or engage in activities on behalf of the school without authorisation from the school Designated Safeguarding Lead, or their deputies or the Directors. The Bursar retains the right to remove or approve content posted on behalf of the school.

3. I will ensure that any content posted abides by copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.

4. I will follow the school's policy regarding confidentiality and data protection/use of images. This means I will ensure that the school has written permission from parents/carers before using images or videos which include any members of the school community. Any images of pupils will be taken on school equipment, by the school and in accordance with the school image policy. Images which include pupils will only be uploaded by the school. These will be for the sole purpose of inclusion on the tool I am using e.g. Facebook, Twitter and will not be forwarded to any other person or organisation.

5. I will promote online safety (e-Safety) in the use of all social media and will help to develop a responsible attitude to safety online and to the content that is accessed or created. I will ensure that the communication has been appropriately risk assessed and approved by a member of senior leadership team/ Designated Safeguarding Lead/head teacher prior to use.

6. I will set up a specific account/profile using a school provided email address to administrate the account/site/page if required and I will use a strong password to secure the account. Personal social networking accounts or email addresses are not to be used. The school Designated Safeguarding Lead and/or school leadership team/head teacher will have full admin rights to the site/page/group.

7. Where it believes unauthorised and/or inappropriate use of the tool being used or unacceptable or inappropriate behaviour may be taking place, the school will exercise the right to ask for the content to be deleted or deactivated.

8. I will ensure that the content and channel is suitable for the audience and will be sensitive in the tone of language used and will ensure content is written in accessible plain English.

9. I will report any accidental access or receipt of inappropriate materials or inappropriate comments to the head teacher and/or Designated Safeguarding Lead urgently.

10. I will ensure that the site/page is moderated on a regular basis as agreed with the school Designated Safeguarding Lead.

***I have read, understood and agree to comply with the School Social Networking***

***Signed:*** ……..……. ***Date*** ...…..……..

***Print*** ……..……..…….....

***Accepted*** ……..……

***Print*** ……..……

HEATHCOTE
Preparatory School & Nursery

# Appendix D

## Staff Acceptable Use Policy 2021

As a professional organisation with responsibility for children's safeguarding, it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites**.**

School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. **To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.**

I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and

symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system and is changed regularly. In many cases users will be using a company provided password to access their systems.

I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager. If I inadvertently do so, I will notify the Headteacher and IT Lead immediately and understand that it is important to do so promptly.

I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely (e.g. via VPN). Any images or videos of pupils will only be used as stated in the esafety policy and will always take into account parental consent.

I will ensure that when if I use personal devices such as laptops to access company systems remotely such as HUBmis, Outlook or Teams, I will protect the devices in my care from unapproved access or theft and only use them for the purposes intended.

I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.

I will respect copyright and intellectual property rights.

I have read and understood the school online safety (e-Safety) policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces

I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to Designated Safeguarding Lead.

I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, then I will report this to the ICT Support Provider/Team/lead (Head teacher) as soon as possible.

My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership team and/or Head Teacher.

I will ensure that my online reputation and use of ICT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media/networking, gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of ICT and internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school AUP and the Law.

I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, or the school, into disrepute.

I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Safeguarding Lead.

Only staff who have read and accepted the Acceptable Use Policy for company social media accounts will interact with, amend or change these, including the company Facebook and Twitter pages.

I understand that my use of the school information systems (including any devices provided by the school), school Internet and school email may be monitored and recorded to ensure the safety of children and staff and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

*The School may exercise its right to monitor the use of information systems, including Internet access and the interception of emails in order to monitor policy compliance. Where it believes unauthorised and/or inappropriate use of the schools information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the school suspects that the school system may be being used for criminal purposes then the matter will be brought to the attention of the relevant law enforcement organisation.*

**I have read and understood and agree to comply with the Staff Acceptable Use Policy.**

Signed: ……..

Print Name: ……

Date: ……

Accepted by: ……

Print Name: ……