HARBOURSIDE LEARNING Partnership

E-safety Policy
Including use of social media and mobile devices

Committee:	A&S Committee
Policy Ratified:	29 January 2019
Review Date:	January 2022

Additional School Procedure	
Committee:	
Procedure Adopted:	
Review Date:	

1. Aims

Schools within Harbourside Learning Partnership (HLP) aim to:

Have robust processes in place to ensure that pupils, staff and volunteers are safe when using IT including when online.

Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology

Help pupils to develop critical thinking skills to reflect and enable them to keep themselves safe.

Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Keep any personal data and information secure and minimise the risks associated with handling sensitive information.

Have a discerning attitude to online content and be sensible with how it is received and interpreted.

1.1 Links with other policies

This policy should be read in conjunction with:

Code of Conduct (for staff, volunteers, governors and trustees)

Safeguarding and Child Protection Policy and Procedures

Partnership-wide Policy for Behaviour and Exclusions and school- specific Behaviour and Anti-Bullying Policy (or equivalent)

Anti- Bullying Policy

Complaints Procedure

Staff disciplinary procedures

Data Protection Policy

Use of Cameras and Images Policy

1.2 Legislation, guidance and scope:

1.2.1 This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education and Inspections Act 2006 and the 2011 Education Act.

1.2.2 The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by

this policy, which may take place outside of school, but which is linked to membership of the school. The 2011 Education Act increased these powers giving teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

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

1.2.4 This policy complies with our funding agreement and articles of association.

1.2.5 This policy applies to all members of the HLP schools' communities (including staff, pupils, trustees, governors, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the schools. It also applies to the use of personal devices where they are used in school or to undertake business of the school.

2. Roles and responsibilities

2.1 The Trust Board

2.1.1 The HLP Trust Board is responsible for ensuring that:

An appropriate and compliant e-safety policy exists which outlines the ways in which each school within the trust will seek to ensure that all members of the schools' communities are kept safe when using IT and online;

Other associated trust-wide policies are appropriately linked to support the delivery of requirements of this policy;

Schools have access to an appropriate body which can provide up to date advice and guidance around compliance issues related to the content of this policy;

Each school has a member of staff designated as 'E-Safety Champion';

There is an Appointed Trustee for Safeguarding and that each school has an Appointed Local Governor for Safeguarding.

2.2 The Local Governing Body

2.2.1 The Local Governing Body (LGB) has overall responsibility for monitoring the implementation of this policy and will meet with key staff to discharge this duty. Primarily, this will require the Appointed Local Governor for Safeguarding and the school's Designated Safeguarding Lead (DSL) to include e-safety within their wider safeguarding remit and focus.

2.2.2 All governors will:

Ensure that they have read and understand this policy

Agree and adhere to the terms on acceptable use of the school's ICT systems and internet

2.3 The Headteacher

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

2.4 The E-Safety Champion

2.4.1 The school's e-safety champion is responsible for:

Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

Ensuring that appropriate training is available for staff

Creating opportunities to educate parents in issues related to e-safety

Promoting e-safety generally through the school

Liaising with other agencies and/or external services if necessary

Providing regular updates on e-safety in school to the Headteacher and/or LGB

Working closely with the school's DSL in ensuring that e-safety arrangements are contributing effectively to overall safeguarding arrangements in the school

Working with the Headteacher, ICT manager (or equivalent) and other staff, as necessary, to review arrangements following any issue or incident related to e-safety in school.

Act as an immediate point of contact for any member of staff of pupil who may have an immediate concern related to e-safety.

2.4.2 This list is not intended to be exhaustive.

In this school, the E-Safety Champion is Derek Wingrove.

2.5 The Designated Safeguarding Lead

2.5.1 Details of the school's Designated Safeguarding Lead and deputy/deputies are set out in the Safeguarding and Child Protection Policy and Procedures.

2.5.2 The DSL will work closely with the e-safety champion and in particular will:

Ensure that e-safety arrangements are effective in their contribution to overall safeguarding arrangements.

Work with the Headteacher, ICT manager (or equivalent) and other staff, as necessary, to address any online safety issues or incidents.

Ensure that any online safety incidents are recorded and dealt with appropriately in line with this policy and other linked policies.

Ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.

2.5.3 This list is not intended to be exhaustive.

2.5.4 In this school, the DSL, Deputy DSL(s) and Appointed Local Governor for Safeguarding are named in the Safeguarding and Child protection Policy and Procedures.

2.6 The ICT manager (or equivalent)

2.6.1 Schools may have an ICT Manager as a contracted member of staff. Alternatively, schools may choose to engage an external organisation to provide this support. Either way, the responsibilities are the same.

2.6.2 The ICT manager (or equivalent) is responsible for:

Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

Ensuring that the school's ICT systems are appropriately secure and that any incidents or breaches are investigated

Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

Supporting key staff (such as e-safety champion, DSL, Headteacher) in investigating any online safety or cyber-bullying incidents.

2.6.3 This list is not intended to be exhaustive.

2.6.4 In this school, the ICT Manager (or equivalent) is Ian Gamlin

2.7 All staff and volunteers

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

Maintaining an understanding of this policy

Implementing this policy consistently

Agreeing and adhering to the terms of acceptable use of the school's ICT systems and the internet (appendix 1c and ensuring that pupils follow the school's terms on acceptable use (appendix 1a and 1b)

Working with the DSL to ensure that any online safety / cyber-bullying incidents are appropriately dealt with in line with this and other associated policies and that such incidents are appropriately logged.

2.7.2 This list is not intended to be exhaustive.

2.8 Parents / carers

2.8.1 Parents/carers are expected to:

Notify a member of staff as most appropriate (such as e-safety champion or child's teacher) of any concerns or queries regarding this policy.

Support the school in its endeavours to prevent and resolve any online safety / cyber-bullying incidents.

Discuss the Pupil Acceptable Use Agreement (appendix 1a or 1b) with their child and so support the school in underlining the importance of that agreement and ensuring that its content is understood.

Ensure that they have read, understood, signed, returned and adhere to the Parent/Carer Acceptable Use Agreement (appendix 1d)

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

NSPCC online safety advice: https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues

Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics

Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

Regular free digital safety magazine for parents: https://www.vodafone.com/content/digital-parenting/parents-and-carers.html

2.9 Visitors and members of the community

2.9.1 Visitors and members of the community can only use the school's ICT and internet with permission from the Headteacher. Where permission is granted, those who use the school's ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 1e).

3. Educating pupils about online safety

3.1 HLP schools follow the 'Computing Programmes of Study' within the National Curriculum and consequently pupils are taught about online safety as part of the curriculum:

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

Use technology safely and respectfully, keeping personal information private

Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

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

Use technology safely, respectfully and responsibly

Recognise acceptable and unacceptable behaviour

Identify a range of ways to report concerns about content and contact

3.4 Additionally at KS2, computing lessons will cover the SWGfL digital literacy lessons of which there are five per year group.

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

3.6 The school will use assemblies and other high-profile occasions (such as the annual Safer Internet Day) to raise pupils' awareness of the dangers that can be encountered online and in social media and will also invite speakers to talk to pupils about this such as Dorset Police 'Safer Schools and Communities Teams'. Such issues are also covered elsewhere in the curriculum including PSHCE.

4. Educating parents about online safety

4.1 Schools will take any opportunity to raise parents'/carers' awareness of internet safety and support parents/carers as they manage their own children's online experiences and behaviours outside of school. Key strategies used by schools will include written communications home (both preventative and educational as well as, if appropriate, in response to emerging local issues and incidents) as well as information readily accessible via schools' websites. This policy will also be made available to parents/carers via schools' websites.

4.2 In addition to the above, schools will work with other partners such as Dorset Police 'Safer Schools and Communities Teams' to facilitate regular opportunities for parents/carers to learn about issues related to e-safety.

4.3 If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with either the e-safety champion or DSL (e-safety champion named on page 3; DSL and any Deputy DSLs named in the school's Safeguarding and Child protection Policy and Procedures available on the website).

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

5. Social networking – pupils and staff

5.1 Social media has a broad definition encompassing all online platforms where individuals are able to interact: that ranges from opinion and image forums such as Twitter and Instagram to more diverse blogging and gaming settings. Social media will be managed in HLP schools with due regard to the major government safeguarding and security guidance on the topic, namely *Keeping Children Safe in Education* (KCSiE) and *The Prevent Duty: Departmental Advice for Schools and Childcare Providers*.

5.2 KCSiE notes that staff/pupil communication terms should be covered in staff codes of conduct as social media can provide a platform for the development of inappropriate and unprofessional relationships between staff and pupils. KCSiE also references the role of social media in the radicalisation of young people, although it is often one of many factors which facilitate susceptibility to extremist ideology. The

Prevent Duty: Departmental Advice for Schools and Childcare Providers states that schools and childcare providers should be aware of the increased risk of online radicalisation as terrorist organisations such as ISIS seek to radicalise young people through the use of social media and the internet.

5.3 Computing lessons as well as other opportunities within the curriculum will include the dangers of social media usage such as grooming, 'fake news' and radicalisation.

6. Pupils' use of social media

6.1 Pupils are taught about the risks associated with internet usage and to conduct themselves sensibly and safely on social media platforms. Under the General Data Protection Regulation 2016, parental consent is required to process the data of children under the age of 16 online where the processing, in an information services context, is reliant on consent. Pupils will be encouraged to adhere to this requirement, as it is designed to protect them online from illegal data collection and processing. HLP schools will not tolerate:

- Cyber bullying and persecution of individuals through abuse and harassment;
- The posting of inappropriate content, including the overtly sexual, or racist, sexist or homophobic opinions;
- The distribution of non-consensual or sexual images; and
- The abuse of staff, school, or aggressive criticism of site practices.

6.2 Incidents will be dealt with in accordance with relevant policies and in equal weight to acts of harassment, bullying, abuse or hate speech perpetrated on site.

6.3 Pupils are encouraged to report concerns and are aware of the channels of support available.

7. Staff Use of Social Media

7.1 The appropriate use of social media is included in the HLP staff code of conduct; all staff are required to understand and adhere to this code.

7.2 HLP schools respect the private life of staff but have a responsibility to protect the reputation of the Trust/school and the safety and wellbeing of employees and pupils. Staff are expected to conduct themselves in a way which reflects positively on the high standards to which the Trust adheres. Staff will be reminded periodically of the expected standards:

- Staff must not risk damage to the school's reputation on social media at work or within their own time. This includes on their own or school owned technology, by criticising or insulting pupils, staff, parents, relevant third parties, figures in the community or the site;
- Staff must not discuss school or trust-related matters through social media, or share confidential information regarding colleagues or pupils;
- Staff must not 'share' or 'like' potentially offensive material or pages, or promote criminal activity;

- Staff must not post content or opinions deemed racist, sexist, homophobic or hateful;
- Staff should not attempt to contact pupils or their parents via social media, or any other means outside school, in order to develop any sort of relationship. They must not make any efforts to find pupils or parents' social media profiles with the intention of engaging through this media. Any correspondence received should be reported to the DSL. The only exception to this would be if a member of staff had a friendship with a family which pre-dated the child joining the school; staff are advised to discuss this with their Headteacher or DSL.

- Staff should not routinely befriend ex-pupils, including through social media. Such befriending is never appropriate if the ex-pupil is still a child (below 18) and beyond this age staff should exercise caution, taking advice from their Headteacher or DSL if uncertain;
    - Staff must not carry out cyber bullying or intimidating behaviour;
    - Staff must not publicise personal conversations, link to personal sites or disclose private emails; and
    - Staff must not post which could be considered inappropriate or offensive.

7.3 It is not appropriate for staff to be accessing social media on school ICT equipment on the school grounds. Such access is also not permitted using personal devices unless it is within agreed break periods and away from areas where there may be pupils.

7.4 Staff are encouraged to report inappropriate behaviour online if they witness, or believe it to be being conducted, by a member of staff. Inappropriate behaviour involving a child or pupils must be reported. The Trust's Whisteblowing policy is available to all staff and outlines how staff can raise concerns.

7.5 Staff are highly advised to have the privacy settings on the highest setting if they choose to have a presence on social media sites. **If staff choose to have a public personal profile on social media sites**, they must not name their specific place of work or employer – this will help protect staff from being 'found' by parents and pupils as well protect the trust/school from reputational risks associated with content on the staff member's site. Additionally, and for their own further protection, staff are advised to not include their full name but consider using a first and middle name instead or ensure that profiles are made private.

7.6 Staff are reminded not to assume their conversations on social media sites are confidential or secure and not to share personal information, such as their home address.

8. Schools who choose to have a school social media account

8.1 Some schools may choose to have their own social media account which is managed and controlled by the school. This is not discouraged as it can be a means to communicate quickly with the community and a platform for the school to promote its work and the achievement of its pupils. It is also a way in which a school can actively demonstrate positive, safe and responsible use of social media.

8.2 If a school chooses to use social media in this way (such as a Twitter or Facebook account, for example), it will have designated staff members who control

and monitor the content and activity of the account; these staff members will ensure that they are highly conversant with this and other associated policies (including 'Data protection' and 'Use of Cameras and Images Policy'). They will ensure that all content is positive and does not risk compromising the reputation of the school, the trust or any member of the school or trust community, including pupils, staff and parents.

8.3 Schools will also be mindful of the following:

8.3.1 Any such account will be carefully monitored by designated staff. This will include monitoring any 'followers' and blocking any who appear to be inappropriate or not in keeping with an education setting.

8.3.2 Designated staff will ensure that access details to the account are kept secure. This includes ensuring that passwords are not 'remembered' by computers and other devices that they may use to access the account as well as changing passwords on at least a termly basis.

8.3.3 Such accounts which usually only post (or 'tweet' or 'blog' etc) between the hours of 8am and 6pm Monday to Friday during term times. Although the account will not routinely be used outside of these times, there may be exceptions such as covering school events (for example residential visits) or sharing urgent school news (eg school closure).

8.3.4 The school account will only 'follow' other accounts which are from recognised and trusted sources such as known artists, authors, public figures and other schools. Designated staff will manage who can be 'followed' and advice will be sought from the Headteacher if there is any doubt.

8.3.5 The school will not routinely reply to comments made against its own posts. This is because such replying can become unwieldy but also because the school will seek to ensure that social media is not used as a platform to discuss or debate school-related issues. Any complaints or other concerns that are found on the account will be referred to the Headteacher for consideration and may well be removed.

8.3.6 The school's use of its social media account will be strictly in accordance with the requirements of other policies, most notably 'Data protection', 'Use of Cameras and Images Policy', 'Code of Conduct for Staff' and the 'Acceptable Use Agreement.' The school should be especially careful in its use of pupils' images which can be used provided that consent has been sought and provided that the image is not used alongside other personal information such as full name.

8.3.7 Swift action will be taken in response to any comments made on social media which risk reputational damage. In terms of staff, this could well be a disciplinary matter. Parents and other members of the community who use social media negatively will be challenged and such posts removed. When registering their child at an HLP school, all parents are required to sign an acceptable use agreement which makes reference to social media as follows: 'I will ensure that any social media comments related to the school are polite and respectful and do not discuss members of staff or children in any negative way.'

8.4 Some schools may find that they are closely associated with a social media account, even though they do not directly control it. One example of this might be a

Parent Teacher Association which chooses to operate such an account in order to plan events and share news. Schools should ensure that they have an open dialogue with the person(s) running this account so that such person(s) are clear about the sort of use and content which is acceptable to the school. Schools should also monitor the activity on such accounts directly so that they have some awareness of the emerging content and can take action as required.

9. Cyber-bullying

9.1 Definition

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

9.2 Preventing and addressing cyber-bullying

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

9.2.2 Schools will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. The issue will be addressed in high-profile opportunities such as assemblies and by engaging with national events such as 'Safer Internet Day' (an annual global event every February).

9.2.3 The curriculum in schools includes opportunities to teach children about issues related to cyber-bullying. This is an element of the computing curriculum but also features within areas such as personal, social, health and economic (PSHE) education, and other subjects where appropriate. Schools will work with other partners such as the Dorset Police 'Safe Schools and Communities Teams' to facilitate regular opportunities for pupils to learning about issues related to e-safety.

9.2.4 The schools' engagement with parents/carers around e-safety issues (as described earlier) includes educating about cyber-bullying: what it is, how it can be identified and reported, how it can be prevented and how it can be stopped.

9.2.5 In relation to a specific incident of cyber-bullying, the school will follow the processes set out in its key policies, particularly Behaviour and Anti Bullying Policies. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavors to ensure the incident is contained.

9.2.6 The DSL will consider whether an incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

9.3 Examining electronic devices

9.3.1 School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including

mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

9.3.2 When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

Cause harm, and/or

Disrupt teaching, and/or

Break any of the school rules

9.3.3 If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

Delete that material, or

Retain it as evidence, and/or

Report it to the police

9.3.4 Any searching of pupils will be carried out in line with the DfE's latest guidance.

9.3.5 The UK Council for Child Internet Safety (UKCCIS)'s guidance 'Sexting in Schools and College: Responding to Incidents and Safeguarding Young People' goes into more details than the DfE's guidance 'Searching, Screening and Confiscation: Advice for Headteachers, School Staff and Governing Bodies'. The UKCCIS guidance (page 15) stresses the importance of adults not viewing youth produced sexual imagery unless there is good and clear reason to do so. It also discusses the importance of getting the Designated Safeguarding Lead (DSL) involved in making decisions. Pages 15-17 of the UKCCIS guidance offers thorough advice, including guidance on referring an incident to appropriate authorities (e.g. social care or police), viewing the imagery and deletion of images. The UKCCIS guidance also includes advice on when to get the police involved, including a bullet point list on page 11.

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

9.3.7 In all cases where any such action has been taken, schools will liaise closely with parents/carers.

10. Acceptable use of the internet in school

10.1 All members of the schools' communities including pupils, parents, staff and volunteers are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1a-d). Visitors will be expected to read and agree to the school's terms of acceptable use if relevant.

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

10.3 HLP schools reserve the right to monitor the websites visited by any users to ensure they comply with the above.

10.4 More information is set out in the acceptable use agreements in appendices 1a-d.

10.5 Section 7 of the HLP Code of Conduct for Staff includes a requirement for 'acceptable use of technology'; all staff must be familiar with and adhere to this code. This e-safety policy extends that requirement to all members of the school community.

10.6 Children are required to engage with the acceptable use agreement on an annual basis. Staff are required to sign the agreement on appointment and thereafter whenever there may be a significant change to it. Parents are asked to sign the agreement when their child joins the school; schools will use other mechanisms such as newsletters to remind parents of the key points within the agreement as appropriate and required.

11. Pupils using mobile devices in school

11.1 Mobile phones are discouraged. If a particular pupil/family feels strongly that a mobile phone is required, perhaps to ensure that the child feels safe walking to and from school, then it must be:

Switched off on arrival into the school grounds

Handed in to an adult according to the school's particular arrangements

Collected at the end of the school day

Turned on only once the pupil has left the school grounds. (Tthere may well be exceptional circumstances where it is reasonable to allow a child to activate their phone on school grounds for example if they have been unable to locate their parent at their usual meeting place).

11.2 Pupils are not usually permitted to bring other mobile devices (wifi-enabled or camera) into school since any equipment required to support learning will be provided by school. There may be some exceptional circumstances where a pupil is permitted to bring technology to school, such as a device with a camera for a school trip. Such exceptions are considered fully in the 'Use of Cameras and Images Policy' but, in summary, any use of mobile device (be it school-owned or personal) must be in line with the acceptable use agreement.

11.3 Devices brought into school and used inappropriately and/or not handed in for safe keeping as required by this policy will be confiscated. Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy.

12. Staff using mobile devices in school

12.1 It is accepted that many staff are extremely likely to have a mobile device in school, such as a mobile phone. This is permitted, but staff must accept responsibility for the security of their device. Staff are not permitted to use their personal device during school hours (unless on designated breaks or other 'non-contact' time such as PPA time) and should not use their personal devices in front of pupils. For example, a personal phone call on a mobile phone can only be made or taken outside of working hours or during recognised break periods and always away from areas where there are pupils. If any staff member has a situation outside of school which they feel may require them to have ready and immediate access to their own personal mobile device, they should discuss this with their Headteacher.

12.2 The only exception to this might be if a member of staff is using a personal device in school specifically as a teaching resource. For example, playing a piece of

music via a mobile phone during a dance lesson. This is accepted provided that the member of staff is entirely and fully compliant with the appropriate use agreement regardless of the fact that it is their own personal device and also that during this time it is ONLY used for the teaching and learning purpose.

12.3 Any use of a personal device in school must be in line with the acceptable use agreement as if it were a school device. Staff must not use their own device to take images of children; further details can be found in the 'Use of Cameras and Images Policy'.

12.4 The use of personal technology in school is covered within the staff code of conduct.

13. Visitors using mobile devices in school

13.1 Under normal circumstances, 'casual' visitors are only permitted to use mobile phones is designated areas and it is for each individual school to determine appropriate designated areas according to local circumstances. For example, it may well be that a school is likely to have no objection to a parent using a mobile phone whilst waiting for their child in a secure reception area; however, a parent could not use their mobile phone whilst walking elsewhere around the school. When outside of designated areas, visitors to the school should have any mobile device out of sight, in bags or pockets. Schools will display clear signage to that effect explaining that this requirement is for safeguarding reasons. Any visitors who need to use their mobile devices will be asked to do so in a designated area or leave the school premises in order to do so. School staff will, however, exercise professional judgement and use of mobile devices may be permitted in certain circumstances for example an anxious parent who needs to access a piece of information to help assist in finding the location of their child.

13.2 Visiting professionals may be permitted to use the school wifi provided that the purpose of their use is restricted to their professional role for example, accessing emails or electronic papers for meetings. Visiting professionals can only use their mobile device in the area where they are working and away from areas where pupils may be found. If a school has a separate 'guest' network, visitors should be granted access to this rather than the main network.

14. Staff using work devices outside school

14.1 Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 1c.

14.2 Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. USB devices must be avoided for transporting sensitive or personal data and, if they are required for any purpose, they must be password protected.

14.3 Work devices are provided to enable staff to fulfil their professional duties and as such should generally be used solely for work activities. If the device is used for any personal use, such as access to the internet including social media, then it must be entirely compliant with the requirements laid out in this policy and in the acceptable use agreement.

14.4 Further detail around this is included in the Data Protection and Use of Cameras and Images policies.

14.5 If staff have any concerns over the security of their device, they must seek advice from the Data Protection Manager and / or ICT manager (or equivalent).

15. How schools will respond to issues of misuse

15.1 Where a pupil misuses the school's ICT systems or internet, or breaks the requirements of the acceptable use agreement in any way, schools will follow the procedures set out in the behaviour and/or other appropriate policy. Any action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

15.2 Where a staff member misuses the school's ICT systems or the internet, breaks the requirements of the acceptable use agreement in any way or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. Any action taken will depend on the individual circumstances, nature and seriousness of the specific incident. In any such incidents, advice will always be taken from the HLP HR Manager.

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

16. Training

16.1 All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. This will include the safe and appropriate use of social networking sites including how staff can use them in a way which protects their professionalism and the reputation of the school.

16.2 All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails and staff meetings) and this is usually provided by the e-safety champion. Schools will ensure that such training is provided by an external organisation such as Dorset Police Safer Schools and Communities Team every other year. Additional training is provided on e-safety and cyber-bullying issues at least every two years by the Dorset Police Safer Schools and Communities Team.

16.3 The DSL and any deputy/deputies will undertake level 3 child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

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

16.5 Volunteers will receive appropriate training and updates, if applicable.

16.6 More information about safeguarding training is set out in the Safeguarding and Child protection Policy and Procedures.

17. Use of cameras and images

17.1 There is a separate policy which details in full HLP schools' arrangements for managing cameras and images. All staff should be familiar with the content of this policy.

18. Data Protection

18.1 There is a separate policy which details in full HLP schools' arrangements for managing data protection and the General Data Protection Regulation. Particularly relevant to this e-safety policy are those sections which highlight security arrangements (such as the need for appropriate password management) as well as arrangements for storing and transferring data.

19. The management and use of email

19.1 E-mail is an essential communication tool which enables school staff to fulfil their professional duties efficiently and which can also facilitate purposeful communications with parents. All staff are required to use only their work email address for their professional duties: it is not appropriate to discuss the business of the school or to communicate with parents through a personal email account or other digital means such as text messaging, social media or chat. Staff and other users of school email should be mindful that e-mail is never completely secure. Sensitive information should not be sent via email unless it is appropriately encrypted. Users must also ensure that email communication is appropriate and professional in tone. Staff should be aware that inappropriate use of email may well invoke the disciplinary procedure.

19.2 Users must immediately report to the Headteacher or the DSL, or in the case of the Central team the CEO, receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature. Such communication must not be responded to. Parents are also required to ensure that their use of email is appropriate and in line with that laid out in the parents'/carers' acceptable use guide (appendix 1d). Parents/carers found to be communicating inappropriately with staff via email will have their email communications dismissed and any material thought to be illegal/threatening/intimidating/harassing may be reported to the appropriate authority.

19.3 Users of the school email system should be aware that this system is monitored and HLP reserves the right to access such communications. Arrangements and circumstances around this are outlined in the data protection policy.

19.4 Pupils at KS2 may be provided with individual school email addresses for educational use. If this is the case, then pupils' use of this facility must be compliant with the acceptable use agreement. They will be taught how to report any communication which is inappropriate or makes them feel uncomfortable. Whole class / group emails may be used at KS1 (and at KS2 if individual email addresses are not given to the pupils). Children will also be taught to have an awareness of digital threat which is often perpetrated by email.

Appendix 1a: Acceptable Use Agreement – KS2 pupils

.Acceptable use of the school's ICT systems and internet:

Agreement for Pupils

Name of pupil:

I will always take care of all school equipment (including computers, cameras and headphones).

I will use school technology for school-related work and with permission from a suitable adult.

I will not knowingly access any inappropriate websites or start any inappropriate online searches.

I will not go on any social networking sites at school (unless an adult has allowed this as part of a learning activity).

I will not use chat rooms whilst I am school.

I will not open any attachments in emails, or follow any links in emails, without first checking with a teacher.

I will not upload or download to and from the school network (including using USB devices).

I will not use any inappropriate or unkind language when communicating online, including in emails.

I will keep my username and password to access the school network safe and secure; I will not try to log in to the school's network using someone else's details or try to access any other person's account or documents.

When researching online, I will do my best to check that information is truthful and accurate and avoid plagiarism (copying).

I will immediately tell an adult if I see any unpleasant or inappropriate materials, or anything which makes me feel uncomfortable.

I will be polite and respectful and not take part in cyber-bullying and report any that I know about as soon as possible.

I will be aware of 'stranger danger' when communicating online and will not share any of my personal information (including my name, address, telephone number, date of birth)

If I bring a personal mobile phone or any other personal device into school:

I will turn it off as soon as I enter the school grounds and hand it in to be kept safe for the day; I will not switch it on again until I leave the school grounds except in an emergency.

If given permission to capture images / videos during a school event with my own device or a school device, I will keep them safe and not share online.

I will not share images of any members of the school community online.

I understand that the school will monitor the websites I visit. I give permission for my work to be celebrated and shared with the school community, including online.	
Signed (pupil):	**Date:**

Appendix 1b: Acceptable Use Agreement – EYFS / KS1 pupils

.**Acceptable use of the school's ICT systems and internet:** ***Agreement for Pupils***	
Name of pupil:	
This is how we stay safe when we use computers: I will ask a teacher or suitable adult if I want to use the computers / tablets I will only use activities that a teacher or suitable adult has told or allowed me to use I will take care of the computer and other equipment I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong I will tell a teacher or suitable adult if I see something that upsets me on the screen I know that if I break the rules I might not be allowed to use a computer / tablet	
Write your name here to show that you have talked about this with an adult at school:	**Date:**

Appendix 1c: Acceptable Use Agreement – Staff, regular external agencies and partners, governors, volunteers

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to assist their work and to enhance learning opportunities for pupils; in return, staff and volunteers are expected to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I will, where possible, educate the pupils in my care in the safe use of digital technology and embed online safety in my teaching.

For my professional and personal safety:

- I understand that the school will monitor my use of the school ICT and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured. (Staff should be familiar with the 'Use of Cameras and Images Policy').

- I will only use social networking sites in school in accordance with the school's policies (on a personal device and only outside of school hours or on official breaks and always away from areas used by pupils)
- I will not communicate with pupils under any circumstances through digital means.
- I will only communicate with parents/carers using official school systems. Any such communication will be professional in tone and manner; I will remember that under GDPR, parents/carers may have a right to request access to email exchanges involving them or about them of their child.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- If I use my own mobile devices (laptops/tablets/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- If accessing work emails, or any other work-related materials, on a personal device, I will ensure that such devices are appropriately password protected.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not try to upload, download or access any materials which are inappropriate or may cause harm or distress to others or which may be illegal (such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act). I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless I have appropriate permissions.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will ensure that I have read and understood the Data Protection Policy and comply with its requirements including those related to the storage and transfer of personal information.
- I understand that data protection policy requires that any staff or pupil data to which I have access will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority for example for safeguarding reasons.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Agreement, I could invoke the school's disciplinary procedures; if my practices are thought to be illegal, this would require the involvement of the Police.
- I will inform the designated safeguarding lead (DSL) and Network Manager (or equivalent) if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

I have read and understand the following policies:

Staff Code of Conduct (or equivalent for governors and other volunteers)

Data Protection

Use of Cameras and Images

E-Safety

Safeguarding and Child Protection Policy and Procedures

Staff / Volunteer Name: .....

Signed: .....

Date: .....

Appendix 1d: Acceptable Use Agreement – Parents / Carers

.Acceptable use of the school's ICT systems and internet:

Agreement for Parents / Carers

Name of child:

This Acceptable Use Agreement is intended to ensure:

That children will be responsible users and stay safe while using the internet and ICT tools

That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

That parents/carers are aware of the importance of online safety and are involved in the education and guidance of children with regard to their on-line behaviour.

That parents are mindful of the impact of their own use of technology on the school community.

I know that my child will discuss and sign an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that children will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet.

I understand that my child's ICT activity will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Agreement.

I will encourage my child to adopt safe use of the internet at home and will inform the school if I have concerns over my child's online safety or the online safety of any other child.

I understand that, if my child brings personal IT devices into school (eg phones, cameras, smartwatches etc), the devices will be collected in, kept safe and returned at the end of the day; they should not be turned on until my child has left the school grounds.

The school's 'Use of Cameras and Images Policy' is on the website. I understand that if I come to have digital images of children other than my own (for example, after taking pictures at a school event), I must not put them online without the explicit consent of the other children's parents/carers.

I agree that any email communication from me to the school will be:

- Related to non-urgent matters;

○ Directed to the right person (eg routine queries straight to the office, not a teacher); ○ Sent at appropriate times of the day / week (eg not to staff at evenings and weekends – emails can be sent at such times but preferably via the school's generic email address for the attention of the relevant teacher); ○ Reasonable in terms of the volume of emails sent; ○ Polite, courteous and respectful in tone; ○ Not demanding of a response in an unreasonable timeframe. I will ensure that any social media comments related to the school are polite and respectful and do not discuss members of staff or children in any negative way.

Signed (parent/carer):	**Date:**

Appendix 1e: Acceptable Use Agreement – Community Users

A**cceptable use of the school's ICT systems and internet:** ***Agreement for Community Users***
Name of person/organisation:

This Acceptable Use Agreement is intended to ensure:

- That community users of school's ICT will be responsible users, stay safe while using these systems and devices and use ICT and internet for purposes appropriate to a school environment.
- That school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That users are protected from potential risk in their use of these systems and devices
- I understand that use of school systems, devices and ICT will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are inappropriate or may cause harm or distress to others or which may be illegal (such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act). I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices
- I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

If you are completing this form on behalf of an organisation, you are personally responsible for ensuring that your members are fully aware of the content of this agreement.

Signed: Name:	Date: