OPOSSUM Federation

Online Safety Protocol

Date : Summer 1 2017-2018
Review Date: Summer 1 2018-2019

Chair of Governors Initials

The Opossum Federation's Online Safety Leaders are also the Designated Safeguarding Lead Professionals; Michele Moir (Dawlish), Nicola Forsyth (Newport) and John Dodd (Thorpe Hall).

- The Online Safety Protocol has been written by federation staff, building on LBWF and government guidance. It has been agreed by staff and school leaders and approved by governors
- The Online Safety Protocol and its implementation are reviewed annually.

Rationale

The Opossum Federation understands the benefits and the risks to young people of using the Internet and this document outlines the procedures we are putting in place to ensure that the children in our care become safer, more discerning users of the Internet and related technologies.

Adults, as well as young people, can find themselves vulnerable to malicious use of the Internet both in their personal and professional lives. This Online Safety Protocol highlights the importance of training and guidance in good practice in safer use of the Internet for staff. The protocol also recognises that there are other safety issues associated with using technologies, such as over-exposure to LCD screens, privacy etc.

The Internet and associated technology is a rapidly evolving environment where new opportunities and risks appear daily. The Opossum Federation teaches young people how to manage existing risks and understand the dynamic nature of technologies, so that they are able deal confidently with challenges in the future, whatever they might be.

Links with Other Policies/Curriculum Areas

- Safeguarding in Schools Policy
- Keeping Children Safe in Education (statutory guidance)
- PSHE curriculum
- Computing Curriculum
- Data Protection policy/GDPR (with particular reference to email guidelines)
- Acceptable Use Agreement
- Home School Agreement
- Anti Bullying Procedure
- Social Media Policy
- EYFS Policy
- Code of Conduct

Rights' Respecting Links

UNICEF Rights' Respecting Article 17: Every child has the right to reliable information from the media. This should be information that children can understand. Governments must help protect children from materials that could harm them.

1. Teaching and learning

As we move towards a more digital curriculum, the Opossum Federation acknowledges and will actively promote the use of 'real-world' technologies as an aid to learning.

1.1 Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. Schools have a responsibility to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

1.2 Internet use will enhance learning

- The schools' Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils (Appendix 1)

- Pupils will be taught the differences between acceptable and unacceptable Internet use and given clear objectives for Internet use.

- The schools are vigilant in their supervision of pupils' use at all times, as far as is reasonable, and common-sense strategies are applied where older pupils have more flexible access.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

- Teachers will update and check websites before accessing with the children to ensure that the content is appropriate. The curriculum is planned in context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. kiddle.co or kidsclick.org

- To promote learners' independence and sense of personal responsibility, pupils in Years 5 and 6 sign an Online Safety/ acceptable use statement/Class Charter which is fully explained and used as part of the teaching programme (Appendix 2).

- Parents provide consent for pupils to use the Internet, as well as other IT technologies, as part of the Online Safety acceptable use agreement form at time of their child's entry to school.

- The schools make clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings, parent workshops and the curriculum plans.

- A record is kept of any cyberbullying or inappropriate behaviour in-line with the federation's behaviour management system. Parents/carers are informed of significant or repeated inappropriate behaviours.

- The Federation ensures the Designated Safeguarding Lead Professionals have appropriate training in Online Safety practice.

- The Federation provides advice and information on reporting offensive materials, abuse/ bullying etc and makes this available for pupils, staff and parents.

- Online Safety advice for pupils, staff and parents is provided.

- The schools ensure that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights.

- The schools ensure that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include; risks in pop-ups; buying on-line; on-line gaming / gambling, in app purchases.

- The schools ensure staff know how to send or receive sensitive and personal data and understand the requirement to protect data through password protection or encryption.

- The schools make training on the Online Safety education programme available to staff as part of the cycle of Safeguarding training.

- The schools run a rolling programme of advice, guidance and training for parents, including:
    - Information leaflets; practical sessions; in school newsletters; on the school web site;
    - distribution of 'think u know' for parents' materials https://www.thinkuknow.co.uk/teachers/resources/
    - suggestions for safe Internet use at home;
    - provision of information about support sites for parents, e.g. CEOP and UK Safer Internet Centre (Appendix 3)

1.3 Pupils will be taught how to evaluate Internet content

- The schools will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- The Opossum Federation has a clear, progressive Online Safety education programme throughout all Key Stages, built on local and national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:
    - to STOP and THINK before they CLICK
    - to discriminate between fact, fiction and opinion;
    - to develop a range of strategies to validate and verify information before accepting its accuracy;
    - to skim and scan information;
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - to know how to narrow down or refine a search;
    - [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
    - to understand 'Netiquette' behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
    - to understand why they must not post pictures or videos of others without their permission;
    - to know not to download any files – such as music files - without permission;
    - to have strategies for dealing with receipt of inappropriate materials;
    - to understand online purchasing e.g. apps and within app purchases
    - [for older pupils] to understand why and how some people will 'groom' others with inappropriate or illegal motives (Appendix 4)

2. Managing Internet Access

2.1 Information system security

- The schools' IT systems capacity and security are reviewed regularly.
- Virus protection is updated regularly.

2.2 E-mail

- Pupils may only use approved school e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters or similar 'spam' is not permitted.

2.3 Published content and the school web site

- The contact details on the Web site are the school address, e-mail and telephone number. Staff, pupil or governors' personal contact information will not be published.
- The Executive Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.4 Publishing pupil's images and work

- Photographs that include pupils will not reference their full name. Digital images /video of pupils stored in a teacher's documents or shared images folder on the network are deleted at the end of the year – unless specifically required for a key school publication or assessment information.
- Images of children and staff are not to be taken on or away from school premises by parents or visitors, unless prior permission is sought and given by the school or at scheduled school events such as assemblies or festivals.
- Pupils are not identified by their full name in online photographic materials in the credits of any published school produced video materials / DVDs.
- Parental agreement is obtained, through the consent form signed at point of admission, before pupils images are published on the school's website or other publications e.g. local newspapers.
- Pupil's work can only be published externally with the permission of the pupil and parents/carers.
- Staff sign the school's Acceptable Use Agreement and this includes a clause on the use of mobile phones/devices and personal equipment for taking pictures of pupils (Appendix 5)
- Images of children and staff are not to be taken on or away from school premises by parents or visitors, unless prior permission is sought and given by the school, or at scheduled school events such as assemblies or festivals (Appendix 6).
- Pupils are taught about how images can be manipulated, and possible implications of this, in their Online Safety education programme and also taught to consider how to publish for a wide range of audiences, which might include governors, parents, peers or younger children.

2.5 Social networking and personal publishing

- The schools block/filter access to social networking sites or newsgroups unless there is a specific, approved educational purpose.
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that networking sites have Terms and Conditions, such as minimum age which must be observed.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind that may identify them or their location, or that of family or friends.
- Pupils and parents are advised that the use of some social network spaces, for example Facebook, Instagram, Twitter, outside school is inappropriate for primary aged pupils and that some of these sites have minimum age requirements.
- Pupils are taught that they should not post images or videos of others without their permission on websites or apps. They are taught about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school, including the use of geolocation permission settings. They are taught

the need to keep their data secure and what to do if they are subject to bullying or abuse (Appendix 7).

2.6 Cyber-bullying

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

- To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
- The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teaching staff are encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
- The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.
- In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will consider whether the 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.

2.7 Examining Electronic Devices

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.
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

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

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.
Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

2.8 Preventing Radicalisation

- Protecting children from the risk of radicalisation should be seen as part of schools' wider safeguarding duties, and is similar in nature to protecting children from other forms of harm and abuse. During the process of radicalisation it is possible to intervene to prevent vulnerable people being radicalised.

- The Internet and the use of social media in particular has become a major factor in the radicalisation of young people.

- As with other safeguarding risks, staff should be alert to changes in children's behaviour which could indicate that they may be in need of help or protection. Staff should use their judgement in identifying children who might be at risk of radicalisation and act proportionately which may include making a referral to the Prevent/Channel programme.

- Schools and colleges must ensure that children are safe from terrorist and extremist material when accessing the Internet in schools.

  Keeping Children Safe in Education (2016) replaced by Revised Guidance 3 September 2018

2.9 Managing filtering

- The school will work with relevant providers to ensure systems which protect pupils are regularly reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Online Safety Leader. Concerns are escalated to the technical service provider as necessary.

- The school will immediately refer any material we suspect is illegal to the appropriate authorities e.g Police, and the local authority.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any breaches of security or filtering failure are logged and actions taken immediately to secure the system.

2.10 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Personal mobile devices will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

2.11 Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) as is currently set out in the Data Protection Bill.

3. Policy Decisions

3.1 Authorising Internet access

- All staff and students (or parents/carers on their behalf) have signed an acceptable use agreement form that requires that they report any concerns.

- The school reserves the right to withdraw Internet access from a pupil or member of staff in the event of misuse or infringement of policy.

3.2 Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor LBWF can accept liability for the material accessed, or any consequences of Internet access.
- The school will review ICT policy, protocols and provision regularly to establish whether the Online Safety protocol is adequate and that its implementation is effective.

3.3 Handling Online Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head of School.
- Complaints of a child protection nature must be dealt with in accordance with schools' child protection procedures.
- Pupils and parents are able to access the Complaints Procedure on the school website or request a hard copy document from the school office.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

3.4 Community use of the Internet

- The school will liaise with local organisations that use school facilities to establish a common approach to e-safety.

4. Communications Policy

4.1 Introducing the Online Safety protocol to pupils

- Online Safety rules are displayed in all classrooms and other work areas and are discussed with the pupils on a regular basis, including during planned curriculum provision
- Pupils are informed that network and Internet use will be monitored.

4.2 Staff and Online Safety

- The Online Safety Protocol is distributed to all staff and is included in the cycle of annual child protection training sessions.
- Internet usage is able to be monitored and can be traced to the individual user. Discretion and professional conduct is essential.
- All staff receive induction into the Online Safety procedures on appointment and have access to update training as part of the programme of professional development.

4.3 Enlisting parents' support

Parents/carers' attention will be drawn to the school Online Safety Protocol in a variety of ways including: newsletters, the school brochure and on the school web site.

Appendix 1

Internet policy and procedures: background information

Owing to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear. **Supervision is the key strategy.** Whatever systems are in place, something could go wrong which places pupils in an embarrassing or potentially dangerous situation. Pupils will be taught how to respond if such a situation arises.

Surfing the Web

- Aimless surfing should never be allowed. It is good practice to teach pupils to use the Internet in response to an articulated need – e.g. a question arising from work in class. Children should be able to answer the question "Why are we using the Internet?"
- Search engines can be difficult to use effectively and pupils can experience overload and failure if the set topic is too open-ended. It is not sensible to have younger pupils 'searching the Internet'.
- Pupils do not need numerous web sites on a topic. A small selection will be quite enough choice, and as with other resources, the teacher needs to have checked and selected them so they are appropriate for the age group and fit for purpose. Favourites / bookmarks or hyperlinks within a document are a useful way to present this choice to pupils.
- Teachers may use Googledrive to provide learning resources for pupils to access outside of school. This service is protected by the security provided by Google. Pupils are taught that the same protection of Googledrive log in passwords is required at home as when they are using the Internet at school.

Search Engines

- Internet search engines are managed through the LGfL provider, this service ensures that appropriate filters and restrictions are put in place to reduce the risk of pupils accessing inappropriate material.
- Copyright rules relating to material sourced on the Internet will be taught as part of the Computing curriculum. Images usually have copyright attached to them which is an issue commonly overlooked but a key teaching point to pupils and staff.

Collaborative Technologies

- There are a number of Internet technologies that make interactive collaborative environments available. Often the term 'social networking software' is used. Examples include blogs (personal web-based diary or journals), wikis (modifiable collaborative web pages), and podcast sites (subscription-based broadcast over the web) supported by technologies such as RSS (really simple syndication – an XML format designed for sharing news across the web). Using these technologies for activities can be motivational, develop oracy and presentations skills, helping children consider their content and audience. Schools are best protected by using the social collaboration tools within the school's Learning Platform, such as the London MLE.
- Blogs: A school may want to use them as a method of online publishing, perhaps creating class blogs, or to creatively support a specific school project. A 'safe' blogging environment is likely to be part of a school's Learning Platform or within LGfL /LA provided 'tools'.
- These are a popular aspect of the web for young people. Numerous sites allow users to share and post web sites, videos, podcasts etc. It is important for children to understand that these sites are public spaces for both children and adults. They are environments that should be used with caution. Users, both pupils and staff, need to know how to keep their personal information private and set-up and use these environments safely. [See Education programme]
- Most schools will block such sites. However, pupils need to be taught safe behaviour as they may well be able to readily access them outside of school. There are educational, monitored services that schools can purchase such as GridClub SuperClubs. Additionally, the LGfL Learning Platform provides a safe environment for pupils to share resources, store files in an ePortfolio, and communicate with others through 'closed' discussions, etc.

Podcasts

- Podcasts are essentially audio files published online, often in the form of a radio show but can also contain video. Users can subscribe to have regular podcasts sent to them and simple software now enables children to create their own radio broadcast and post this onto the web. Children should be aware of the potentially inappropriate scope of audience that a publicly available podcast has and to post to safer, restricted educational environments such as the LGfL. Podcast central area. http://www.lgfl.net/SERVICES/CURRICULUM/Pages/Podcasting.aspx

Chatrooms

- Many sites allow for 'real-time' online chat. Children should only be given access to educational, moderated chat rooms. The moderator (or referee) checks what users are saying and ensures that the rules of the chat room (no bad language, propositions, or other inappropriate behaviour) are observed. Pupils should be taught to understand the importance of safety within any chat room because they are most likely at risk out of school where they may access chatrooms.

Sanctions and infringements

- The Online Safety/Acceptable Use policy is made available and explained to staff /governors, pupils and parents, and acceptance/agreement forms are completed appropriate to their age and role. Failure to comply with the Acceptable Use Agreement may result in sanctions applied from the school's pupil behaviour policy or staff discipline policy (as appropriate).

- Incidents relating to Child Protection will result in referrals to external agencies such as, the police, LADO and Children's Social Care.

Appendix 2

Acceptable Use Agreement for KS2 Pupils

The Internet and associated technology is a rapidly evolving environment where new opportunities and risks appear daily. The Opossum Federation teaches young people how to manage existing risks and understand the dynamic nature of technologies, so that they are able deal confidently with challenges in the future, whatever they might be.

Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Rules for Online Safety

1. I agree to keep my mobile telephone number and address, the name/location of my school and my parents' work address/telephone number private.
2. I agree to report any information, images, messages or websites that make me feel uncomfortable or upset to my parents or my teacher.
3. I will never agree to get together with someone I "meet" online unless it is part of my class learning and has been organised by the school.
4. I will never send a person my picture or anything else without first checking with my teacher.
5. I will never respond to any mean or unkind messages. I will tell my parents/teacher if any messages make me feel uncomfortable, upset or unhappy
6. I will follow my teachers' rules for going online about the time of day, the length of time and appropriate sites to visit.
7. I will never give out school Internet passwords to anyone (even my best friends) other than my teachers.
8. I will always check before downloading or installing software or doing anything that could possibly hurt the computer/device or jeopardize my school's privacy.
9. I will be a good online citizen and not do anything that hurts other people or is against the law.
10. I will help my parents understand how to have fun and learn things online. I will teach them about the technology I am using.

KS1 Agreement

Appendix 3: Internet use - Possible teaching and learning activities

A range of resources and activities are available through CEOP – Child Exploitation and Online Protection

http://www.thinkuknow.co.uk/5_7/

https://www.thinkuknow.co.uk/Teachers/Lee-And-Kim/

http://www.thinkuknow.co.uk/8_10/

https://www.thinkuknow.co.uk/teachers/resources/?tabID=2

https://www.thinkuknow.co.uk/parents/

The UK Safer Internet Centre also contains valuable information for teachers and parents

https://saferInternet.org.uk/

Appendix 4

Top Tips for Teachers & School Staff

Keeping kids safe and happy using ICT

1. If an inappropriate site or image is accessed, play the situation down. Always report the incident immediately to the e-safety co-ordinator or headteacher. Ensure that it is recorded.
2. Don't assume it is the pupil's fault, once blamed a pupil may never confide again.
3. Monitor use of chat rooms, social networking sites and mobile phones for inappropriate use.

4. Encourage pupils to report inappropriate use of mobile phones, email or Internet by either bullies or adults.

5. Be vigilant when asking pupils to search for images. Always test an image search before demonstrating in class.
6. Remind pupils that all downloads must be linked to curriculum work.
7. Ensure that pupils cannot be individually identified in website images.
8. Ensure protection of teacher and administrator passwords. Never leave machines that are logged on unattended.
9. Regularly remind pupils of key e-safety messages such as "never give out personal details online".

If you need any further information or advice, please ask the school's e-safety co-ordinator

LONDON GRID FOR LEARNING

LGFL in association with CEA@islington

CEA@Islington

Appendix 5

Acceptable Use Policy (AUP): Staff Agreement Form

- Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.
- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body. I will not reveal my password(s) to anyone.
- If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will ensure all data are saved, accessed and deleted in accordance with the school's network, data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities, including use of social media.
- I will only use the approved, secure email system(s) for any school business (currently: lgflmail.org)
- I will only use the approved school email or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business. I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to or receipt of inappropriate materials, or filtering breach to the appropriate line manager / School Business Manager.
- I will report the loss or theft of hardware such as laptop, tablet to the Head of School/School Business Manager as soon as possible.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's Online Safety curriculum into my teaching.
- I will only use LA systems in accordance with any corporate policies.

- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request for example in the event of an allegation that requires investigation.
- I understand that failure to comply with this agreement could lead to disciplinary action.

User Signature

- I agree to abide by all the points above.
- I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent Online Safety policies.
- I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

Signature Date ....

Full Name (printed) .....

Job title .....

School .....

Authorised Signature (Executive Head Teacher/Head of School)

- I approve this user to be set-up.

Signature ..... Date.....

Full Name (printed) .....

The school is registered in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) as currently set out in the Data Protection Bill. The school is required to share some of the data with the Local Authority and with the DfE.

Appendix 6

Pupil Image Protocol

The following information is drawn from the schools' Online Safety protocol and Safeguarding Policy.

Photographs and video footage are very useful tools for recording children's learning in the moment and progress over time. Images are regularly used across the school and very frequently in the Early Years Foundation Stage (EYFS) to capture examples of children's achievements, interactions with their peers and the world around them.

The following protocol is in place within the school to ensure appropriate use and storage of pupil images.

- Parents/carers are asked to sign consent forms during the admission process to enable staff to take photos and videos of their children in the setting and for publication, for example on the school website. This consent may be withdrawn at any time by contacting the school in writing.
- Staff are aware of pupils who have not been granted photographic consent.
- Photographs and videos are taken by staff using password protected school devices such as ipads which are owned by the school.
- Staff sign the school's Acceptable Use Agreement, which includes a clause on the use of mobile phones/devices and personal equipment for taking pictures of pupils.
- Images may be used to record learning experiences, as an assessment tool or to celebrate achievements in display.
- In the EYFS, photos may be linked to the child's profile using the school's electronic assessment system; photos are also used in children's 'Special Books'.
- Staff always ensure pupils are appropriately dressed.
- Staff encourage pupils or their parents to tell us if they are worried about any photographs that are taken of them
- Pupils are not identified by their full name in online photographic materials or in the credits of any published school produced video materials.
- Digital images /video of pupils stored in a teacher's documents, email or shared images folder on the network are deleted at the end of the year – unless specifically required for a key school publication or assessment information.
- Images of children and staff are not to be taken on or away from school premises by parents or visitors, unless prior permission is sought and given by the school.

Appendix 7

SMART thinking

S	**Safe** STOP and THINK Will the information you share keep you safe?
M	**Meeting** STOP and THINK Are your online friends who they say they are?
A	**Accepting** STOP and THINK How do you know files and pictures are safe?
R	**Reliable** STOP and THINK How do you know that people or pages aren't lying?
T	**Tell** STOP and THINK Who can you tell if you feel uncomfortable about something online?