Oakdene Primary School

in association with

St.Helens Council

Online Safety Policy

Policy Adapted by: M.Weston

Date reviewed: May 2018
Date to be reviewed: Jan 2020

Ratified by Governors …… (Signed)
…… (Date)

Schedule for Monitoring

The implementation of this Online Safety policy will be monitored by the:	Senior Leadership Team
Monitoring will take place at regular intervals:	At least annually
The Governors Sub Committee will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Annually
Should serious online safety incidents take place, the following external persons / agencies should be informed:	LA Safeguarding Officer, LADO, Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Surveys / questionnaires of
    - pupils
    - parents/carers
    - staff

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Head teachers 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 the school but is linked to membership of the school.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate Online Safety behaviour that take place out of school.

1. Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

1.1 Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Sub Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator
- reporting to relevant Governors

1.2 Head Teacher and Senior Leaders

- The Head Teacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.
- The Head Teacher and Deputy Head Teacher should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority disciplinary procedures).
- The Head Teacher and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Head Teacher and Senior Leaders will ensure those in school who carry out the internal online safety monitoring are also monitored and supported.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Officer Lead.

1.3 Online Safety Lead

- Consults regularly with other members of the school community (e.g. pupils through pupil voice; parents through surveys and internet safety workshops) to ensure knowledge and application of online safety is current.
- Takes day-to-day responsibility for online safety issues and has the leading role in establishing and reviewing the school online safety policies
- Ensures that all staff be aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Maps and ensures provision of the online safety curriculum provision throughout school (yearly plans from Gooseberry Planet to be used from September 2018).
- Provides relevant and up-to-date training and advice for staff
- Liaises with the Local Authority
- Liaises with school technical staff (Agilisys)
- Receives reports of online safety incidents and keeps a log of incidents to inform future online safety developments

- Communicates with the Online Safety Governor to discuss any current issues as necessary
- Attends relevant meetings of Governors and reports to the Senior Leadership Team
- Communicates with and monitors parents in terms of their access to Gooseberry Planet for online safety information.

1.4 Technical staff

The staff from Agilisys (in alliance with the subject leader for Computing, and the school office manager) is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required online safety technical requirements and any Local Authority Online Safety Guidance that may apply.
- Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- Filtering is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network/internet/remote access/email is regularly monitored in order that any attempted misuse can be reported to the Head Teacher or Online Safety Lead for investigation
- That monitoring systems are implemented and updated as agreed in school policies

1.5 Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices.
- They have read, understood and signed the Staff Acceptable Use Agreement (AUP).
- They report any suspected misuse or problem to the Head Teacher or Online Safety Lead for investigation – this can be done using Safeguarding Monitor.
- All digital communications with pupils, parents or carers should be on a professional level and only carried out using official school systems (e.g. school texting service or school email address for communication with parents; relevant forum and blog comments for communication with pupils on School Spider).
- Online safety issues are embedded in all aspects of the curriculum. From Autumn 2018, Gooseberry Planet will be used to inform teaching content of online safety.
- Pupils understand and follow the Online Safety Policy and Internet Use Policy for Pupils (see Appendix).
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor the use of digital technologies in lessons and other school activities (where allowed) and implement current policies with regard to these devices.

- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

1.6 Designated Safeguarding Lead

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

1.7 Pupils

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the taking / use of images and on cyber-bullying.
- Understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

1.8 Parents / Carers

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet in an appropriate way. The school will take every opportunity to help parents understand these issues through access to the Gooseberry Planet subscription service. This will be implemented in September 2018 and parents will receive a log-in. This should inform them of relevant and up-to-date national online safety campaigns, literature and issues. Further newsletters, letters and workshops will be arranged as necessary to supplement the information on Gooseberry Planet.

Parents and carers will be encouraged to support the school / academy in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events – a form will be signed to declare that any images will not be used inappropriately for social media/sharing etc.
- Access to parents' sections of the school website

1.9 Community Users

Community Users who access school systems as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

Policy Statements

2.1 Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited. From autumn 2018, this will be through the Gooseberry Planet subscription service, which provides a set of lessons for every year group and which is regularly updated to include the most relevant content.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and activities.
- Pupils should be taught in all lessons to be critically aware of the content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies and the internet.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

2.2 Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Access to Gooseberry Planet log-in and subscription service (from September 2018), giving up to date information on online safety, as well as a representation of their child's performance in lessons linked to online safety
- Further information via the school website, letters and newsletters, or parent workshops
- Safer Internet Day promoted in school.

2.3 Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's / academy's online safety knowledge and experience. This may be offered through the following:

- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community.

2.4 Education & Training – Staff / Volunteers

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

- A planned programme of formal online safety training will be made available to staff via staff inset sessions. This will be regularly updated and reinforced. An audit of the online safety training needs will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school / academy Online Safety Policy and Acceptable Use Agreements.
- Some staff may identify online safety as a training need within the performance management process.
- The Online Safety Lead or Computing subject leader will receive regular updates through attendance at external training events (eg from Knowsley/Oaks Teaching Alliance) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to staff.
- The Online Safety Lead will provide further guidance or training to individuals as required.

2.5 Training – Governors

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

- Attendance at training provided by the Local Authority or other relevant organisations.
- Participation in school information sessions for staff or parents
- Updates as required in governors meetings related to important changes to online safety.

3.1 Technical – infrastructure / equipment, filtering and monitoring

Agilisys, in conjunction with the school and local authority, will be responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible, and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a group log-in and password by Agilisys. For the school website and other subscription services, users will be provided with an individual username and password (provided by the Computing subject leader). Users are responsible for the security of their username and password and should alert staff if they feel the security of their log-in information has been compromised. *See Appendix for Authorisation and Removal of Access forms*
- The office manager and Agilisys technician are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (e.g. when apps have been purchased).
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- Teachers and office staff have access to allocated school devices (laptops and iPads). Staff members should not download and install executable files or programmes/apps on school devices. This should be raised as a request to Agilisys through the sthelens.org.uk portal and a technician will complete this request. The exception to this policy is for free apps which can be installed on to staff iPads using Apple log-ins via the Apple store, as long as their purpose is educational.
- When working off-site, staff members should use JUNOS to access the school network remotely on their devices. One Drive may also be used for file storage.

- Any pen drives/memory sticks used must be encrypted and password protected. Personal data cannot be sent over the internet or taken off the school site. It is highly recommended that pen drives and memory sticks are not used.

3.2 Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include cloud based services such as email and data storage. All users should understand that the primary purpose of mobile devices in a school context is educational.

- The school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*No*	*Yes*[2]	*Yes*[2]
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only				*No*	*No*	*No*

School-owned laptops and tablets (iPads) are allocated to teaching staff members, as outlined in the technical section above. The usage of these devices is outlined in the section below (Internet Use)

3.3 Internet Use

Head Teachers should critically consider the granting of Internet access to ensure that usage will add value to the member of staff's role in the School. Head Teachers should also ensure that all members of staff are aware of the need for this authorisation before attempting to use the Internet and that any unapproved connection may constitute a breach of the Code of Conduct. The Head Teacher should maintain a list of staff authorised to have access to the Internet and advise Agilisys so that correct user lists are maintained. An authorisation form must be completed for each member of staff (Appendix 1). A copy of

[1] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

[2] These devices are not allowed in classrooms and should only be kept and used in the staff room or outside the school building unless express permission has been granted by the head teacher or other senior leader in exceptional circumstances.

this should be forwarded to Agilisys. A copy should also be kept on a file at the school for each member of staff granted access. Head Teachers should immediately request the removal of Internet access for leavers and for any member of staff suspended from work. This information should also be made available to Agilisys (Appendix 2).

i) The following rules must be adhered to when using the internet in school:

- Internet access is provided to schools through the St Helens MAN (Metropolitan Area Network). This infrastructure provides an Internet firewall and a filtering mechanism, presently installed at either school or LEA level. Members of staff should not attempt to circumvent or disable any of these features.
- Members of staff should use their individual username and password when accessing the Internet and should not allow other staff to use their usernames.
- When logged onto their Internet account, members of staff should not leave a workstation unattended unless it is locked.
- All connections to the Internet, from within school, must be made through the school network.
- Members of staff should not use, or try to use, a school Internet account for intentionally accessing, displaying, storing or transmitting material that is obscene, sexually explicit, pornographic, racist, defamatory, hateful, incites or depicts violence, or describes techniques for criminal or terrorist acts or otherwise represents values which are contrary to School policy.
- Where access to such sites occurs accidentally this should be immediately reported to the Head Teacher or Online Safety Lead.
- Members of staff must be aware of, and abide by, current GDPR regulations as its provisions cover data transmitted and stored on e-mail. (See the Data Protection Policy and Code of Practice for further details). Except where this is strictly and necessarily required by the job, for example Education where sexually explicit information is accessed to be used in the education/teaching of pupils. The Head Teacher should note all such reported incidents on the appropriate form (Appendix 3) to include the date, time, user and site(s) accessed. Head Teachers, on receiving such information, should contact Agilisys and the site be added to the list of restricted/filtered sites.
- Only those members of staff who are duly authorised by the Governing Body may publish content on electronic forums, upload software or data belonging to the School (e.g. school website, school Twitter account).
- The downloading or purchase of software must be subject to prior authorisation, and in accordance with the school's financial regulations. All software should be properly licensed and registered.
- The downloading of entertainment software, games, music or screen savers (other than for legitimate teaching purposes) is not allowed. Where legitimate downloading takes place it must not breach the rights of copyright owners.
- Any orders placed via the Internet must first be authorised through the normal school financial procedures and in accordance with Financial Regulations.
- The playing of games against an opponent via the Internet is forbidden unless it forms part of a school-purchased educational app (e.g. Sumdog, Mathletics).

- Users should not use, or try to use, the Internet to break through security controls (i.e. hacking).
- Users should not do anything which is illegal under English law or the law of any other relevant country.
- Users should not use, or try to use, a Council/School Internet account for political lobbying.
- Users should not use, or try to use, the Internet to intentionally access or transmit computer viruses or similar software.
- Any software or files downloaded via the Internet becomes the property of the School.
- E-mail users have a duty of care to protect the School, in accordance with the Code of Conduct, from any legal action for the likes of defamation, harassment, libel etc. resulting from staff use of the system.
- Care should be taken when in receipt of unsolicited e-mail as it could be a vehicle for introducing viruses.
- Care must be taken over the content of e-mails. It is important that the inclusion of personal information and of personal references to pupils should be avoided wherever possible. Under Data Protection Legislation, in the event of a Subject Access Request, personal data stored on e-mail is classed as relevant data and must be disclosed to the data subject. The word CONFIDENTIAL should be used in the subject box of emails for any necessary correspondence.
- In exceptional cases, where personal data is transmitted, appropriate security measures must be used (eg. Encryption). Agilisys can advise schools of the most appropriate method. All e-mails will carry the following disclaimer.

'This e-mail and any file transmitted with it are confidential, subject to copyright and intended solely for the use of the individual or entity to whom they are addressed. It may contain privileged information. Any unauthorised review, use, disclosure, distribution or publication is prohibited. If you have received this e-mail in error please contact the sender by reply e-mail and destroy and delete the message and all copies from your computer.'

ii) Members of staff are only allowed private use of the Internet in schools if permission has been granted by the Head Teacher. The basis for such use is that:

- All usage is governed by this Policy as outlined in Paragraph 3 *Rules governing Internet Use.*
- Access must be in the individual's own time and not in school time.
- Personal use must be confined to viewing or browsing. There must be no storage of information, images, software etc.
- There must be no interaction (e.g. shopping, entering competitions, use of credit cards, financial services etc).
- If permission is granted to send private e-mails using the 'sthelens.org.uk' accounts then they should be clearly labelled as being private and not being sent as an official communication from and on behalf of the Council/School. The Council/School will not be held responsible for any fraudulent actions.

iii) Teachers in school are allocated school devices (a laptop and an iPad) which can be taken out of school. It is recognised that when using such school laptops and tablets within their own home, staff will have greater freedom in relation to activities such as on-line shopping. When members of staff are using such equipment for personal use at home the following rules apply:

- Members of staff should not use, or try to use, the Internet for intentionally accessing, displaying, storing or transmitting material that is obscene, sexually explicit, pornographic,racist, defamatory, hateful, incites or depicts violence, or describes techniques for criminal or terrorist acts or otherwise represents values which are contrary to School policy.
- Where access to such sites occurs accidentally this should be reported to the Head Teacher or Online Safety Lead as soon as possible.
- Members of staff must be aware of, and abide by, current data regulations (GDPR) as its provisions cover data transmitted and stored on e-mail. (See the Data Protection Policy and Code of Practice for further details).
- Only those members of staff who are duly authorised by the governing body may publish school content on electronic forums or upload software or data belonging to the School (e.g. web pages, application data).
- Any downloaded software should be properly licensed and registered. The downloading of music or data must not breach the rights of copyright owners.
- Users should not use, or try to use, the Internet to break through security controls (i.e. hacking).
- Users should not do anything which is illegal under English law or the law of any other relevant country.
- Users should not use, or try to use, the Internet to intentionally access or transmit computer viruses or similar software.
- Only the member of staff to whom the computer has been loaned may use the computer to access the Internet. Allowing other family members or friends to use school equipment to access the Internet is not allowed.

iv) Monitoring of internet usage

Members of staff should be aware that Internet access in school is logged by a filtering system and that logs indicating the number and types of web sites that have been accessed by members of staff are subject to review by the Head Teachers and senior leaders. Members of staff using school equipment to access the Internet at home should be aware that the Council's Audit team may, from time to time, make requests for computer equipment to be made available to them for analysis/investigation. Members of staff should be aware that this will not just occur when inappropriate use has been proved, or is suspected but on a random basis. Members of staff should be aware that all Internet activity, using the 'sthelens.org.uk' e-mail accounts, are constantly monitored for inappropriate language. Use of other e-mail accounts will be monitored through random sampling as outlined in the paragraph above. Any inappropriate access/attempts to access, or e-mail activity will be investigated and may lead to disciplinary action being taken against members of staff. Disciplinary action may take the form of Gross Misconduct/Misconduct depending on the severity of the breach of the policy. Any inappropriate access of a

criminal nature will be reported to the Police, or any other relevant agencies that the LEA deems appropriate.
There should be no expectation of privacy in Internet or e-mail usage by individuals.
The School reserves the right to inspect any and all files stored in private areas of the network or on disc in order to assure compliance with this policy.
In line with council strategy all logs of Internet usage are kept for 6 months.

3.4 Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press.
- In accordance with guidance from the Information Commissioner's Office, parents/ carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy, and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere, that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupils' work can only be published with the permission of the pupil and parents or carers.

4. Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.
The school must ensure that:

- It has a Data Protection Policy – see this policy for greater detail.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO).
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice. (see Privacy Notice section in the appendix)
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff members receive data handling awareness / data protection training and are made aware of their responsibilities.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data, or are 'locked' if they move away from them for any period of time.
- Transfer data using encryption and secure password protected devices.

It is recommended that no personal data is stored on any removable device such as a pen drive or memory stick.

5. Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their disadvantages:

	Staff & other adults			Pupils				
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school		■						■
Use of mobile phones in lessons				■				■
Use of mobile phones in social time		■						■
Taking photos on mobile phones / cameras				■				■
Use of other mobile devices e.g. tablets		■					■	
Use of personal email addresses in school or on school network			■					■
Use of school email for personal emails			■					■
Use of messaging apps		■						■
Use of social media		■						■
Use of blogs		■				■		

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

- Any digital communication between staff and students / pupils or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. It is recommended that the school email address is used when communicating with a parent via email. Personal email addresses, text messaging or social media must not be used for these communications.
- Agilisys will be contacted should email addresses be required for pupils to teach part of the Computing curriculum. They will advise the best course of action to take according to current local authority policy.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website.

6 Social Media - Protecting Professional Identity

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However some games, for example Minecraft or Roblox, and video sharing platforms such as You Tube have social media elements to them.

Oakdene Primary School recognises the numerous benefits and opportunities which a social media presence offers. Staff members are actively encouraged to find creative ways to use social media and pupils are taught about the benefits within the online safety curriculum. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by Oakdene's staff, parents, carers and children.

This policy is subject to the school's Codes of Conduct and Acceptable Use Agreements.This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the school.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education

The school respects privacy and understands that staff and pupils may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

6.2 Professional & Personal Communications

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Digital communications with pupils are also considered. Staff should only communicate with pupils via the appropriate comment sections on the school website (School Spider), for example if setting and responding to homework digitally.

6.2 Roles & Responsibilities

- **SLT**
  - Facilitating training and guidance on Social Media use.
  - Developing and implementing the Social Media policy
  - Taking a lead role in investigating any reported incidents.
  - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
  - Receive completed applications for Social Media accounts
  - Approve account creation
- **Administrator / Moderator**
  - Create the account following SLT approval
  - Store account details, including passwords securely
  - Be involved in monitoring and contributing to the account
  - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)
- **Staff**
  - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
  - Attending appropriate training
  - Regularly monitoring, updating and managing content he/she has posted via school accounts
  - Adding an appropriate disclaimer to personal accounts when naming the school

6.3 Process for creating new accounts

The school community is encouraged to consider if a social media account will help them in their work, e.g. school Twitter account, or a "Friends of the school" Facebook page. Anyone wishing to create such an account must present a business case to the School Leadership Team which covers the following points:-

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

6.4 Monitoring

School accounts must be monitored regularly and frequently. Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

6.5 Behaviour

- The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media, staff must contact the head teacher or other senior leader before responding.
- Unacceptable conduct (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

See Appendix for Do's and Don'ts of Social Media advice.

6.6 Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

6.7 Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.
- *See Appendix for Parents, Carers & Visitors Code of Conduct: Use of Social Media*

6.8 Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

6.9 Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts.
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

6.10 Personal use

- **Staff**

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

- **Pupils**
  - Staff members are not permitted to follow or engage with current or prior pupils/students of the school on any personal social media network account.
  - The school's education programme should enable the pupils to be safe and responsible users of social media.
  - Pupils are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy

- **Parents/Carers**
  - If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.
  - The school provides information to parents (via a Gooseberry Planet log-in from September 2018), which supports the safe and positive use of social media. This also includes information on the school website.
  - Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

6.11 Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process (obtain Local Authority guidance).

7 Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school / academy and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be

inappropriate in a school context, either because of the age of the users or the nature of those activities. Oakdene believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	

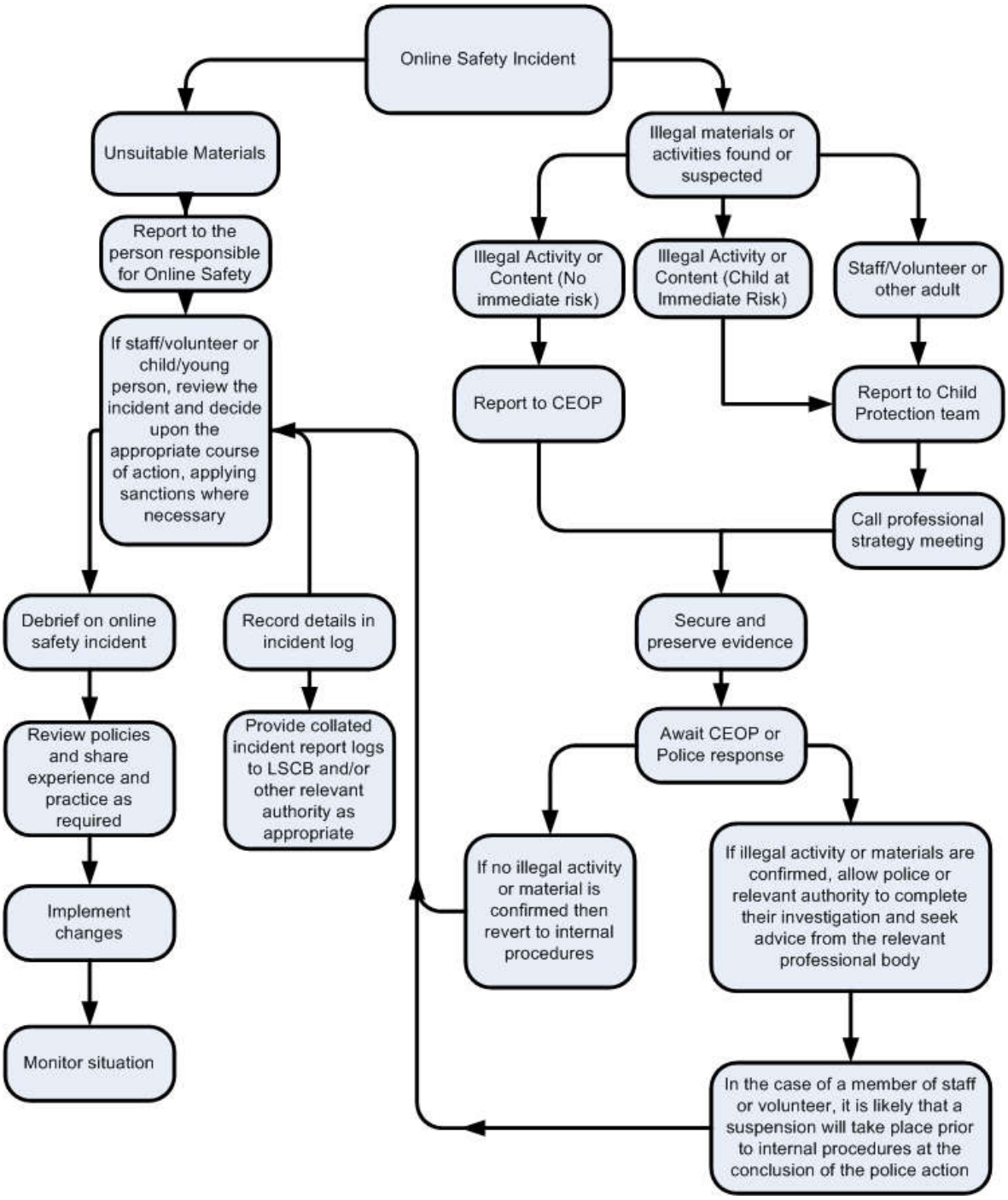
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		X			
On-line gaming (non-educational)			X		
On-line gambling				X	
On-line shopping / commerce				X	
File sharing			X		
Use of social media			X		
Use of messaging apps		X			
Use of video broadcasting e.g. Youtube			X		

8 Responding to incidents of misuse

This guidance is intended for use when staff members need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

8.1 Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

8.2 Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

8.3 School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

	Actions / Sanctions								
Pupil Incidents	Safeguarding Monitor	Refer to Key Stage leader	Refer to Head teacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Move down the behavior ladder	Further sanction e.g. reflection
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons		X						X	
Unauthorised / inappropriate use mobile device		X	X			X			X
Unauthorised / inappropriate use of social media / messaging apps / personal email	X					X			X
Unauthorised downloading or uploading of files		X			X			X	
Attempting to access or accessing the school network or other educational subscription services, using another pupil's account					X	X			X
Attempting to access or accessing the school network, using the account of a member of staff					X	X			X
Corrupting or destroying the data of other users					X	X	X		X

Sending an email or message that is regarded as offensive, harassment or of a bullying nature	X		X			X			X
Continued infringements of the above, following previous warnings or sanctions	X		X	X		X			X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X		X			X			X
Accidentally accessing offensive or pornographic material and failing to report the incident	X				X	X		X	
Deliberately accessing or trying to access offensive or pornographic material	X		X			X	X		X

Actions / Sanctions

Staff Incidents		Refer to Headteacher/Senior Leader /Online Safety lead	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Disciplinary Action		
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email		X						
Unauthorised downloading or uploading of files		X						
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X						
Careless use of personal data e.g. holding or transferring data in an insecure manner		X						
Deliberate actions to breach data protection or network security rules		X				X		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X				X		

Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X				X		
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X						
Actions which could compromise the staff member's professional standing		X						
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy		X				X		
Accidentally accessing offensive or pornographic material and failing to report the incident		X						
Deliberately accessing or trying to access offensive or pornographic material		X				X		
Breaching copyright or licensing regulations		X						
Continued infringements of the above, following previous warnings or sanctions		X		X		X		

Appendix 1

AUTHORISATION OF INTERNET/E-MAIL USAGE

Name

Post Held

Authorisation is granted for Internet/E-mail use in accordance with the Online Safety Policy adopted by the school.

I have read and understand the policy and agree to access the internet/e-mail system in accordance with the policy.

Signed

Printed Name

Date

Authorised by Head Teacher

Date

Appendix 2

NOTIFICATION OF
REMOVAL OF INTERNET/E-MAIL ACCESS

Name

Post Held

Date Access is to Cease

I can confirm that I have notified Agilisys of the above.

Authorised by Head Teacher

Date

Appendix 3

NOTIFICATION
INADVERTENT ACCESS TO INAPPROPRIATE INTERNET SITES

Name

Post Held

Site Accessed

Date of Access

Time of Access

Reported by

I can confirm that I have notified Agilisys of the above.

Authorised by Head Teacher

Date

Part 2

Oakdene Primary School
Internet Use Policy for pupils

I will only access the system with my class login name and password.

I will not access other people's files, or damage their work and data.

I will only use the Internet when I have permission and am supervised by a teacher.

I will use the Internet only for activities and work set by school.

I will only e-mail people my teacher has approved, and not use the Internet for private messages.

I will respect the privacy of others. I will not publish their names, addresses, phone numbers or photographs.

I will not give my home address or telephone number, or arrange to meet someone, through the Internet.

I will not use work from the Internet as if it was my own. I will give credit to the sources of materials included in my work.

I will not try to find or use unacceptable material from the Internet.

I will report any unpleasant material or messages sent to me. I understand this report would be confidential and would help protect other pupils and myself.

I will not use school resources to subscribe to any goods or services, nor buy or sell using the Internet.

I will not download software from the Internet unless this is authorised by the teacher.

I will not bring in disks, CD's or electronic data from outside school unless I have been given permission.

I will not send unsuitable emails or comments in blogs. The messages I send will be polite, responsible and signed in my name.

I will not send anonymous messages.

I will not take part in any activity that goes against school rules or government legislation.

I understand that the school may check my computer folder or log-in to school subscription services

and may monitor the Internet sites I visit.

Remember that access is a privilege, not a right and that access requires responsibility!

Sanctions
Any breach of this policy may lead to the following sanctions:

1. A temporary or permanent ban on Internet use.

2. Pupils' parents being contacted.

3. Other external agencies being contacted.

Oakdene Primary School
Web Site Policy

1. The Headteacher will have editorial responsibility for the school Web site and will ensure that content is accurate and the quality of presentation is maintained.

2. The Web site will comply with the school's guidelines for publications.

3. There will be no link between photographs and individual pupil information.

4. Only images of pupils in appropriate dress will be used.

5. No personal information relating to pupils will be included on our Web site (e.g. email addresses or phone numbers).

6. The point of contact on the Web site will be the school address, telephone number and email address.

7. Information, work or photographs produced by or relating to pupils will only be used if parental permission has been given.

Name of Child…….
Class……..

I will adhere to the School Internet Policy.

Signed (Child)…….

I acknowledge receipt of the Internet and Web site Policy.

Signed (Parent)…….

Appendix

Managing your personal use of Social Media:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

Managing school social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Consider turning off tagging people in images where possible

The Don'ts

- Don't make comments, post content or link to materials that will bring the school into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

Oakdene Primary School

Parents, Carers and Visitors Code of Conduct: Use of Social Media

Over recent years social media tools have become an integral feature of modern life, providing opportunities for organisations (both public and private sector) and citizens to engage and communicate. A key feature of many social media tools is their unparalleled ability to broadcast and receive information quickly and link to a whole network of people in a matter of seconds. It is also the case that material broadcast via eg: Facebook and Twitter can persist in the digital world almost indefinitely often reaching a wider audience than the author had originally intended.

As a public body and regulated setting, responsible for the care and education of children, x School is committed to the responsible and appropriate use of social media. Its own use of social media is governed by its adoption of St Helens Council Social Media Policy (March 2011) itself informed by the Cabinet Office: Participation Online Guidance for Civil Servants (June 2008).

Social media tools include, but are not limited to:

- Blogs\Microblogging
- Social Networking
- Collaboration Networking Media
- Social Bookmarking
- Photo and Video sharing
- RSS Aggregation Services

This guidance forms part of Oakdene Primary School's code of conduct for parents, carers and visitors and seeks to extend those principles to the digital world. It is not intended to stifle legitimate debate, discussion or interfere with private use of social media tools. It aims to:

- Clarify expectations about the use of social media tools by parents, carers or visitors as it relates to Oakdene Primary School.
- Outline the steps Oakdene Primary School will take if it considers social media content to be offensive, inappropriate, inaccurate or otherwise unacceptable.

- Protect the reputation of Oakdene Primary School and ensure that social media use supports its educational, spiritual and pastoral ethos.

- Support the use of existing School policies and procedures to resolve issues of concern.

As part of its code of conduct for parents, carers and visitors Oakdene Primary School expects the following standards to apply in the use of social media tools:

- Foul, abusive, discriminatory or threatening material about the School, its staff or pupils will not be tolerated. Parents\carers posting such material will be contacted by the School for its immediate removal. Whenever necessary the School shall seek legal advice on any further action that might be necessary.

- If parents\carers become aware of offensive/abusive or factually innacurate postings about Oakdene Primary School it is requested that these are brought to the attention of headteacher or member of School staff at the earliest opportunity.

- Oakdene Primary School has policies and procedures for a wide range of issues including bullying, attendance, additional needs and complaints. As such, social media tools are not an appropriate vehicle for progressing such matters. Schools will not engage with parents\carers via this route but will direct parents\carers to the appropriate procedure.

- When factually incorrect information is posted about Oakdene Primary School via social media, the author(s) will be contacted by the School for its removal\correction.

- Oakdene Primary School has a safeguarding duty to all of its pupils and will take appropriate action if it considers social media contents to compromise this. This can include the identification of a child through social media discussion and the use of visual material within content.

Legislation

Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.
It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This

wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harrassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices and for DfE guidance - http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:
https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)