Oak Trees Multi Academy Trust

e-Safety Policy

Issue Status: -

Date	Issue	Comment	By
25.09.18	A		TL

	Signature	Name	Date
Prepared:	Author	Tony Lacey	25.09.18
Verified:	CFO	Claire Jackson	25.09.18
Approved:	Chair of Trustees	Jane Owens	25.09.18

Contents

Appendices:

1 Introduction to e-Safety

The term e-Safety covers the issues relating to young people and staff and their safe use of the Internet, mobile phones and other electronic communication technologies. This policy assesses the protocols for ensuring that these initiatives are carefully developed in our Academy, so that we progress responsibly and appropriately in the interests of our children. It also looks at how we educate our children to be safe in a world where technology is so readily available.

At each Academy we celebrate the value and importance of technology in our children's learning. The internet has become a vital source of learning and communication for all members of our school community.

Pupils interact with new technologies and the Internet on a daily basis and experience a wide range of opportunities and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial but can occasionally place young people in danger.

Our Academy seeks to provide the right balance between controlling access, setting rules and educating students for responsible use.

1.1. Effective Practice in e-Safety

E-Safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and pupils;
- A comprehensive, agreed and implemented e-Safety Policy;
- A well thought out approach regarding how to develop e-Safety guidance within the school's curriculum.
- Identified opportunities to ensure that we support families with the challenges relating to e-Safety in the digital age (family workshops, web-links etc).
- Secure, filtered broadband from Exa Networks and Surf Protect;
- A school network that complies with the National Education Network standards and specifications;
- Staff members in each Academy know their responsibilities in accordance with 'Keeping Children Safe in Education' (DfE 2018) to safeguard children and report abuse immediately to designated staff members, as per the Trust's Child Protection Policy;
- Each Academy will nominate an e-safety officer who will be a member of the Senior Leadership Team and a Governor with responsibility for e-safety to implement the e-safety policy and ensure it is disseminated to staff.

ACADEMY	E-SAFETY LEAD	E-SAFETY GOVERNOR
CHURCH DRIVE		
EGREMONT		
GREAT MEOLS	**Ben Parker**	**James Gaskin**
POULTON LANCELYN		
STANTON ROAD		

1.2 E-Safety and the Legal Issues

E-safety should be applied to protect children, staff and all members of our Academy community. All staff members have a 'duty of care' to ensure that students are educated about e-safety, know how to reduce risk of harm and stay safe, are able to report abuse and know who to talk to about any concerns around the use of this technology. There is also a duty to ensure that staff conduct does not bring into question their suitability to work with children.

E-Safety encompasses not only Internet technologies but also electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet's communication infrastructure internationally. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. Pupils must also learn that publishing personal information could compromise their security and that of others.

Oak Trees MAT make it clear to pupils, staff and visitors that the use of our Academies' equipment for inappropriate reasons is "unauthorised". We will also ensure that all reasonable actions have been taken and measures put in place to protect users.

In practice this means that this Academy ensures that;

- It has effective firewalls and filters on all school networks.
- Ensures that e-Safety responsibilities are clearly communicated to all members of our Academy community.
- That our e-Safety policy is fully enforced for children, staff and visitors.
- Ensures that our procedures are consistent with the Data Protection Act (1998) and GDPR (2018).

2 Learning and Teaching in the Digital Age

The Academy uses a range of devices and comprehensive broadband access to develop learning and teaching through digital communication. Access to instant messenger services and mobile phones is not allowed as part of this school's curriculum. However, the school will include provision to educate children how to use this technology appropriately and safely.

E-Safety is integrated into the Academy curriculum in every circumstance where the internet or technology are being used, and during PSHE (Personal, Social, Health Education) lessons where personal wellbeing is being taught.

Children will be made aware about the possible risks and dangers that they might encounter when using ICT, the internet, mobile phones, gaming stations and personal devices through ICT lessons, implicitly throughout the curriculum and in PSHE. This will include understanding how photographs can be manipulated, the importance of keeping personal information private, information about safe social networking and chat rooms, ownership of personal images, sexting and healthy relationships, awareness of CSE and the implications of inappropriate posts and images on career progression and employment, as well as many other topics.

2.1 Why the Internet and digital communications are important

Mobile Communication equipment and the Internet are an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. We also recognise that children are actively engaged with digital communication from an early age. It is part of their lifelong learning experiences and habits. However, we also have a responsibility to ensure that our children learn to use these opportunities and resources responsibly, appropriately and productively to enhance their learning.

In addition, use of the Internet is a part of the statutory curriculum and a necessary tool for staff and pupils.

2.2 Encouraging responsible use of the Internet and digital communication

a) The Academy Internet access is designed expressly for pupil use and will include filtering appropriate to the age of pupils. This is arranged through Exa Networks and the use of Surf Protect. This service is managed by Hi Impact.
b) Pupils will be taught about responsible and appropriate information sharing through the internet and other forms of digital communication.
c) Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
d) Pupils will be taught about responsible use of e-mails and other sources of digital communication including e-mail, messenger services and texts.
e) Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. When possible, we encourage the use of a school-safe search such as http://www.safesearchkids.com/
f) Pupils will be shown how to publish and present information to a wider audience safely and responsibly.

2.3 Pupils will be taught how to evaluate Internet and other digital communication content

There is a multitude of information available online and it is important that students learn how to evaluate internet content for accuracy and intent. Students are taught to become digitally literate across the whole curriculum and are encouraged to be critically aware of materials they read, and how to validate information before accepting it as accurate. Students will be taught to understand the bias of web authors, separate fact from fiction and practice etiquette on the internet, emails and social media. Students learn how to use age-appropriate tools to search for information online, how to acknowledge the source of information used and to respect copyright. Pupils will be taught how to report unpleasant Internet or other digital content including messages, e-mails and texts.

3 Professional Expectations

The use of computer systems without permission or for purposes not agreed could constitute a criminal offence under the Computer Misuse Act 1990.
Staff members at each Academy are adults and as such should act responsibly and with an awareness of the consequences of their actions. Staff members must act with the best interests of students at all times. This is demonstrated in the following ways:

a) Staff who are provided with a laptop or tablet by the Academy must use this only for academic purposes, these remain the property of the Academy and open to scrutiny by Senior Leaders.
b) All staff members are responsible for their personal use of social media, networks and electronic device and are expected to ensure that any use of such technologies does not breach the Trust Social Media Policy or undermine the reputation of the Academy and Trust.
c) Trust staff are personally responsible for the security and privacy settings when using social media and networks and failing to ensure that privacy settings are secure could lead to a disciplinary process if the content breaches professional expectations.
d) Trust staff must ensure that their use of ICT and social media is professional at all times, even if this is outside of the Academy day, and that behaviour which breaches the Trust's code of conduct could lead to disciplinary action.
e) All contact made with students must be made through appropriate channels and should be made within clear and transparent professional boundaries and only made with regard to matters regarding the Academy.
f) Trust staff must not give out personal details, such as telephone numbers, email addresses, social media identities to students, ex–students or parents/carers of students. Great caution should be advised with regards to any contact with any ex – students and staff members must use their personal judgement and be mindful of their professional standing.
g) Safe and professional behaviour of Trust staff online will be discussed at staff induction training. This relates to the use of social networking sites outside of the working environment. As a Trust employee, it is important to be aware that posting information or views about the Trust or Academy cannot be isolated from your working life. Comments about the Trust or Academy, students, parents/carers or colleagues can bring the Trust and Academy into disrepute and make both the Academy and the employee liable to legal action.

3.1 Appropriate computer usage

a) Staff members are expected to use computers in lessons only for teaching and learning and not for other Academy work.
b) Trust staff should ensure that students are unable to access activities and information on the computers that is not relevant to teaching and learning and the lesson.
c) Staff should log off or lock their computer when not in use to protect confidential and personal information.
d) Students should not use computers in classrooms without permission or without a member of staff being present to ensure that staff members are able to supervise online access and secure equipment.
e) Any misuse or damage to computers in classrooms should be reported to technicians immediately.
f) Staff may be liable to pay for any damage caused by themselves to Academy equipment intentionally or accidently. Each circumstance will be dealt with individually by the Headteacher.

g) Only IT Technicians should move computer equipment, unplug cables or remove screws or covers from equipment and upload/download or copy programs and change, or attempt to change the configuration of any computer. However, staff are able to action updates to software.

3.2 Social media and networks

a) Staff members should not be in contact with students, ex- students in full time education or parents/carers of students using social media and networking, unless prior permission has been given by the Headteacher or you have known them previously on a personal level before they started at the Academy.
b) Students should not be added as friends and staff must not respond to friend requests. If a member of staff suspects that an existing friend is a student or a student is using another name to befriend the member of staff the friendship should be ended and this should be reported to the Headteacher.
c) If a member of staff coincidently has a contact established with an ex-student, parent/carer or student the member of staff must use their judgement and regulate this contact. If a student, ex-student or parent/carer persistently attempts to befriend a member of staff this should be disclosed to the Headteacher.
d) The use of personal social networking activity is at the discretion of the individual, however the professional responsibilities of the individual need to be considered in all postings on this sites.
e) It is important to ensure that your personal information is secure and that high strength passwords are used and that profile settings are restricted. It is advisable to log out of social networking sites when not in use as a security precaution.
f) Staff must be aware of how to set privacy settings on their profile and be mindful that some social networking sites revert to default settings when an update is made to their service. Staff should be vigilant to any changes in their profile privacy settings.
g) Professionals should consider what information they use for their profile, for example the photograph and the amount of personal information that is displayed. Profiles should not identify your employer or place of work.
h) Staff should not publish their Academy email address on a personal social networking site, or use this address as part of your login/registration on a personal site.
i) All postings on social media and networks should be considered to be in the public domain so staff members should consider this when making decisions about the content of social media activity.
j) Any material which is posted on social media and networks which is considered to bring the Trust and Academy into disrepute or is considered to put students or staff at risk of harm will be dealt with under the Trust's Disciplinary Procedure and follow the Allegations Management Policy.
k) Staff members should not make reference online to any students, parents/carers, colleagues or to any work related issue. This also includes posting photographs or videos online which identify your place of work, or any students and parents/carers.
l) While access to social media sites through the Academy network is blocked to employees, accessing the internet through mobile phones and other mobile devices is prohibited during working hours. Staff members should never use Academy networks or equipment to access or update a social media site.

3.3 Facebook and Twitter advice

Facebook and Twitter are media that can have enabled families and friends to stay in contact and have lessened geographical divides, it is important, however that this media is used appropriately. To ensure that staff are safe and protected as professionals:

- Keep your profile picture post modest. Remember students can still search for you and see your picture without being your friend.
- Create your photo albums with privacy settings so 'only your friends' can see them.
- Reject all friend requests from students. You do not need to report this unless it becomes a recurring problem. People are not notified when you reject their friend request.
- Use the Facebook/Twitter privacy settings to limit who can see your full profile. Set it so that only friends can see everything like your pictures, your wall, and your personal and contact information.
- Use limited public information about yourself on your profile. For example, address, email, date of birth, contact telephone numbers do not need to be shown to everyone, they can be privately messaged if needed.
- Do not use your Academy email address as your email contact.
- Do report any threats of violence or other inappropriate posts/images to Facebook or to the relevant authorities, such as CEOP (Child Exploitation and Online Protection centre) or the police.
- Customise your privacy settings. Limit what people can see when you 'poke' or message them before you have added them as a friend. The default setting allows people who are not friends whom you 'poke' or message to see your entire profile.

3.4 The use of mobile phones and personal devices

a) Under no circumstances should staff use their own personal devices to contact students or parents/carers either in or out of Academy time.

b) Staff are not permitted to take photos or videos of students. If photos or videos are being taken as part of the Academy curriculum or for a professional capacity the Academy equipment will be used. Any device which takes images, videos, moving images should not be used during working time as this breaches safeguarding and child protection responsibilities.

c) Any breach of the Trust E-safety and Online Policy may result in disciplinary action against that member of staff. More information on this can be found in the Child Protection Policy and Allegations Management Policy.

3.5 Inappropriate material

In law there is a distinct difference between material that is inappropriate and that which is illegal, however accessing of inappropriate material is a significant concern with regards to safeguarding. Staff should be aware that the accessing of illegal material will lead to a case investigation, allegations management procedures, a possible criminal investigation, prosecution and barring, even if there is no criminal prosecution.

3.6 Illegal material

It is illegal to make, possess or distribute indecent images of a person under the age of 18 and viewing these images online may constitute possession even if they are not saved. Accessing indecent images of children or students on the internet or making, storing or distributing such images of students or children is illegal and if proven could

lead to criminal investigation and the individual being barred from working with students.

3.7 Materials which incite hate, harm or harassment

There are a range of offences in relation to incitement of hatred on the basis of ethnicity, gender, sexual orientation, gender identity religion and beliefs and offences concerning harassment and threatening behaviour which include cyber bullying, whether this is carried out on a mobile phone, social networking or through email. It is an offence in law to send indecent, offensive harassing or threatening messages which cause the recipient distress. Hate crime is a matter for the police and they must be called if a child or member of staff is victim to a hate crime.

3.8 Professionally appropriate material

Trust staff should not use any equipment belonging to the Academy to access adult pornography and equipment with links and images on personal equipment should not be brought into the Academy.

Trust staff should be aware that actions outside of the Academy which are not professionally appropriate and which fundamentally breach the staff code of conduct could result in disciplinary action. Examples of inappropriate materials and actions which breach trust and confidence in professionals are:

- Posting offensive, harassing threatening or bullying comments about colleagues on social networking sites
- Making derogatory comments about students, colleagues, the Academy or Trust
- Posting unprofessional comments about one's profession
- Making inappropriate statements or using offensive or hate based language.

3.9 Confidentiality and Data

Members of staff have access to confidential information about students, other staff and parents/carers in order to undertake their daily duties, this may sometimes include highly sensitive information. This information must not be shared outside of the Academy or with external parties unless a student is at risk of harm or significant harm or there is an agreed multi-agency plan around a family and student.

Confidential information should only be stored on Academy systems and email should never be used to transfer sensitive and confidential information. In such cases, sensitive and confidential information should only be shared using secure methods of communication.

3.10 Cyberbullying

Cyberbullying, bullying, harassment, defamatory comments, offensive correspondence and hate incidents within and outside the Academy will not be tolerated and any member of staff found to be behaving in this manner towards colleagues will be dealt with in accordance with the Bullying and Harassment Policy and in specific circumstances will be considered as a criminal offence.

If any member of staff is a victim of this behaviour they must follow the Whistleblowing Policy and report this behaviour as soon as possible to their line manager or Headteacher. The victim will be offered support and this will be fully investigated and the Bullying and Harassment Policy followed, a referral may be made to the appropriate authorities if deemed appropriate.

3.11 Academy email accounts, etiquette and appropriate use

a) Staff must only use their own Trust account internet and email password, and not share this password.
b) Email etiquette should be observed and emails should be written carefully and politely, the tone of an email should be considered before sending. Emails should be sent to specific member/s of staff and not just a general distribution list, unless applicable and should have a specific title related to the content. Content of emails should be simplified into simple bullet points as much as possible and the 'High importance' feature should be used only if a matter is urgent. Staff should try and respond to email requests as efficiently as possible, however, where possible staff are encouraged to have more face-to-face communication with colleagues.
c) To ensure that we create a professional environment the sending of anonymous messages and chain letters is not allowed.
d) If an email is received with an attachment it must not be opened unless the sender is known. If in doubt, check with the IT Technicians.

4 Managing Digital Access, Communication and Content

4.1 Information system security

Academy ICT systems security, virus protection and security strategies will be reviewed regularly by High Impact Consultancy.

4.2 Managing filtering

a) The Academy will work with Exa Networks and National Bodies to ensure system to protect pupils are reviewed and improved.
b) We understand that we are required "*to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering*".
c) The Academy's filtering system is compliant with the Department for Education's revised statutory guidance 'Keeping Children Safe in Education' in May 2016 (and active from 5th September 2016) for schools and colleges in England. Amongst the revisions, we are obligated to "*ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system*" however, the Academy will "*be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding*."
d) If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety lead who will notify Hi Impact.

4.3 Online Communication

a) Pupil use of e-mail accounts is prohibited. However, children can use class / school blogs under the guidance of Academy staff.
b) In online communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
c) Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
d) The forwarding of chain letters is not permitted.

4.4 Published content and the school web site

a) Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office or a senior member of staff.
b) The head-teacher of each Academy will take overall editorial responsibility and ensure that content is accurate and appropriate.

4.5 Social networking and personal publishing

a) Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
b) Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

4.6 Managing video-conferencing & webcam use

a) Video-conferencing should use the educational broadband network to ensure quality of service and security. Video-conferencing for pupils can only take place under the direct supervision of a member of staff for educational purposes. Examples may be conferencing with another school in India.
b) All software for webcam use will be password protected (Skype etc).
c) The Academy would always seek consent from parents for any video-conferencing. (see appendix 3)

4.7 Managing emerging technologies

a) Emerging technologies will be examined for educational benefit and potential risks will be considered before use in school is allowed.
b) Staff are not allowed to video or take photographs of children using mobile phones as the data is not easily transferrable and may breach our obligations under the Data Protection Act.
c) Visitors are also informed of this as part of our safeguarding statement.
d) Parents can use them for recording only based on the guidelines above. (see appendix 5)
e) Staff are allowed to have mobile devices in school but these must not be used during working hours except for school or emergency based communication in office areas, the staffroom and PPA room.
f) Pupils are not allowed mobile phones or mobile devices (such as ipods, games machines). Accessing the Internet via wireless can bypass school filtering systems and present a new route to undesirable material and communications. Children can bring mobile phones to school in exceptional circumstances and the phone must be named and kept in the school office.
g) Personal mobile devices will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
h) Staff will be issued with a school mobile phone where contact with pupils is required or school camera to capture photographs of pupils. Staff must not take photographs on their personal phones. Guidance @ Children, Families, Health and Education Directorate page 7 June 2008. **See mobile phone policy in appendix 7 for further details.**

4.8 Protecting and storing sensitive data including images

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and GDPR 2018. This information will be clearly communicated to all staff, including office staff on an annual basis.

Staff are aware that they have a professional responsibility to ensure the following;

a) All laptops must be password protected. Work laptops cannot be used for the storage of any inappropriate material.
b) All data and images of children must be stored in the staff shared area on the curriculum network or the school's secure administration network.
c) Photographs cannot be stored on personal laptops.
d) No data or images can be transported out of the school without the device being approved or password protected.

5 Policy and guidance for the safe use of photographs

The Data Protection Act 1998 and GDPR 2018 affects our use of photography. This is because an image of a child is personal data for the purpose of the Act and it is a requirement that consent is obtained from the parent of a child or young person under the age of 18 years (or the child him or herself if deemed competent from 12 years old as suggested by the Information Commissioner) for any photographs or video recordings for purposes beyond the school's core educational function. (E.g. school web sites, school productions). Academy schools seek permission for all photography and video use.

There will also be times where the Academy will be carrying out off-site activities e.g. educational visits and residentials. Our guidelines are created to make sure that all images are taken appropriately by both adults in the school and children taking part in visits.

For both school setting and other events which are photographed for publicity purposes, additional consent should be sought from the child's parent/guardian and kept on file, covering all cases where images of children are to be published beyond the parameters of school use.

Where children are 'Looked After' schools must check consent on the corporate parent's behalf with the social worker and there may be other situations, (in adoption placements or following a resettlement from domestic violence for example), where a child's security is known by the class teacher to be at stake, indicating the need for extra care.

Consent gained for photographs or videos may not extend to webcam use, so it is important to check, when introducing such technology, the status of existing consent for pupils or models.

Consent is sought for the whole time that children are at ********** Primary School. Parents retain the right to withdraw consent at any stage, but they need to do so in writing. On occasions, specific consent is sought to use images/videos on Twitter.

5.1 Publishing pupils' images

a) Photographs that include pupils will be selected carefully. The Academy will always risk assess/review photographs for possible abuse.
b) Pupils' full names and other personal details will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.
c) Written permission from parents or guardians will be obtained before photographs of pupils are published.

d) Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories Guidance @ Children, Families, Health and Education Directorate page 6 June 2008

5.2 Planning photographs of children

Images and details of pupils published together allow for the remote possibility that people outside the school could identify and then attempt to contact pupils directly. The measures described below should help to minimise the risk of such unsolicited attention.

a) Where possible, use general shots of classrooms or group activities rather than close up pictures of individual children.
b) Use images of children in suitable dress, and take care photographing PE events to maintain modesty, using team tracksuits if appropriate for example. Photographs should not be taken of swimming pool based events.
c) Remember to include images of children from different ethnic backgrounds in your communications wherever possible, and positive images of children with disabilities to promote your school as an inclusive community, and to comply with the Disability Discrimination Act.
d) Decide whether parents and visitors will be permitted to take photographs of the event. This must be authorised.

5.3 Identifying children

If the pupil is named, avoid using their photograph. If the photograph is used, avoid naming the pupil.

It is our policy that;

a) You use the minimum information. Ask yourself whether it is really necessary to accompany a picture with the pupils' names, the year group, or the school.
b) When ***fully*** naming pupils in any published text, whether in the school's brochure, website, or in the local press, avoid using their photograph, unless you have parental consent to do so.

5.4 Using photographs of children supplied by a third party

When using third parties, it is our Academy's responsibility to check that the adults are aware of the school protocols. In addition, we would expect that the adult taking the images has a full DBS or is supervised when taking images by a member of the school's staff.

Children should never be left alone with a photographer.

Copyright does not apply to images for private family use. However, copyright does exist in commercial photographs and it rests with the photographer. Copyright is a right that the photographer automatically enjoys as the creator of the work to prevent other people exploiting his or her work and to control how other people use it.

5.5 Use of Images of children by the Press

(Please refer to the recommendations in section 5.3 above; 'Identifying children')
There may be occasions where the press take photographs at school of pupils. If this occurs we will ensure that specific permission is sought from the parent about whether to agree to their children being featured in the press and whether their full name

should accompany the photograph. It is likely that the press will not publish a photograph without the child's name.

5.6 Videos

The Academy will ensure that parental consent is in place before any child can appear in a video. Parents can make video recordings of nativity plays and other such events for their own personal and family use, as they are not covered by the Data Protection Act.

5.7 Websites

Web use can be of particular concern to parents and staff because of the potential misuse of images by paedophiles. With digital photography there is the remote possibility that images of children could be produced, manipulated and circulated without the parents or children's knowledge. The dual concern which follows such a risk is that children might be exploited and a school or setting might be criticised or face legal action. Images on websites can be made more difficult to copy by several measures - copy-protection, overlaying with a watermark, or published in low definition.

It is important to take care with identification and to respect parental views on the use of any photography of children on a website.

Increasingly adults and children are generating content for websites e.g. children and adults placing pictures on **Facebook** and **Twitter**. It is therefore important that schools/organisations ensure that children, staff and parents understand the risks involved and are encouraged to adopt safe practice when generating content for school related websites.

This is included on our permission forms. Parents and staff are not allowed to share school images on any Internet sites.

5.8 Parental right to take photographs and videos

We want parents to have the opportunity to record school events safely and responsibly.

We will allow recording, unless we feel that the images created may be inappropriate (for example a swimming gala). We also have to ensure that consent is gained for all children taking part.

Parents are not covered by the Data Protection Act 1998 if they are taking photographs or making a video recording for **their own private use**. The Act does not, therefore, stop parents from taking photographs or making video recordings at school events, such as nativity plays or other such performances.

Parents are not permitted, however, to take photographs or to make a video recording for anything other than their own personal use (e.g. with a view to selling videos of a school event). Recording and/or photographing other than for private use would require the consent of the other parents whose children may be captured on film. Without this consent the Data Protection Act 1998 would be breached.
(See appendix 4)

5.9 Images taken by young people

Children do have permission to take photographs on days out and residential trips etc. We will ensure that children understand that photographs must be responsible and not taken in private places. For example, in bedrooms or toilets.

6 Developing Our Policies on E-Safety

6.1 Authorising Internet access

a) All staff must read and sign the 'Staff Code of Conduct for ICT' (see Appendix 1) before using any school ICT resource.
b) The Academy will maintain a current record of all staff and pupils who are granted access to school ICT systems.
c) At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
d) All Parents/Guardians will be asked to sign and return a consent form.
e) Any person not directly employed by the school will be expected to follow this policy if needing to access the internet from the school site. This includes governors, student teachers etc.

6.2 Assessing risks

a) The Academy will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the Academy network. The trust cannot accept liability for any material accessed, or any consequences of Internet access.
b) The Academy should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

6.3 Handling e-Safety complaints

a) Complaints of Internet misuse will be dealt with by a senior member of staff.
b) Any complaint about staff misuse must be referred to the head-teacher.
c) Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
d) Pupils and parents will be informed of the complaints procedure (see complaints policy)
e) Pupils and parents will be informed of consequences for pupils misusing the Internet.
f) Discussions will be held with the Police Youth Crime Officer to establish procedures for handling potentially illegal issues. Children, Families, Health and Education Directorate page 8 June 2008

6.4 Community use of the network and Internet

a) Through extended schools use and partnership with other organisations there will be wider community use of the school's network. The Academy will liaise with local organisations to establish a common approach to e-Safety.
b) All consent forms must be used for these groups.

7. Communicating the E-Safety Policy

7.1 Introducing the e-Safety policy to pupils

a) E-Safety will be embedded in computing lessons and will incorporate materials from CEOP.

b) E-Safety rules will be posted around school and discussed with pupils regularly as part of computing lessons.
c) Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
d) E-Safety training will also come into the Personal Social and Health Education (PSHE) curriculum.

7.2 Staff and the e-Safety policy

a) All staff will be given the Academy e-Safety Policy and its importance explained.
b) Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
c) Staff are encouraged to use a child friendly safe search engine when accessing the web with pupils.

7.3 Enlisting parents' and guardians' support

a) Parents' and guardians' attention will be drawn to the Academy e-Safety Policy on the web site.
b) The Academy will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

8 Protecting Personal Data

The Trust believes that protecting the privacy of our staff, students and parents/carers and regulating their safety through data management, control and evaluation is vital to each Academy and to individual progress.

Each Academy collects personal data from students, parents/carers, and staff and processes it in order to support teaching and learning, monitor and report on student and teacher progress, and strengthen our pastoral provision.

Each Academy takes responsibility for ensuring that any data collected is used correctly and only as is necessary, and the Academy will keep parents/carers fully informed of how the data is collected, what is collected, and how it is used.

National Curriculum results, attendance, assessment data, registration records, SEND data, and any relevant medical information are examples of the type of data that the Academy will capture. Through effective data management we can monitor a range of provisions and evaluate the wellbeing and academic progression of students to ensure that they receive an outstanding education and to respond to the changing needs of students.

In line with the Data Protection Act 1998 and the Trust's Data Protection Policy, we will follow the principles of good practice when processing data. Each Academy will ensure that data is fairly and lawfully processed and only for limited purposes. The Academy will ensure that all data processed is adequate, relevant, accurate and not excessive. Data will only be kept for the period of time that is necessary. It will be processed in accordance with the data subject's rights and will always be secure and not transferred to other countries without adequate protection.

There may be circumstances where the Academy is required either by law or in the best interests of our students or staff to pass information onto external authorities; for

example, our Local Authority, Ofsted, or the Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

9 Equal Opportunities

The Trust believes that it is essential that everyone can have access to ICT and that opportunities are provided for all students, regardless of ethnicity, beliefs, values, religion, gender, culture, physical and mental difficulty. This is underpinned by the requirements set out in the Equalities Act 2010.

10 Special Educational Needs and Disabilities (SEND)

ICT can be a positive tool for students with SEND and access to the internet and ICT is a vital link for communication with the outside world and other students, which can allow every student to have access to information, communicate with others and develop ideas and research independently.

11 Consequences of Inappropriate Actions by Staff Members

The Trust may exercise the right to monitor the use of the Academy computer systems, including access to websites, the interception of email and the deletion of inappropriate materials, without the consent of the staff member.

12 Appendices

The following appendices are included as a guide to all Oak Trees schools. However, it is up to each individual school as to whether they use the same proformas or they wish to use the ones which already work well for their individual setting.

Appendix 1

Agreed Staff Code of Conduct to promote e-Safety and Responsible Use

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-safety policy for further information and clarification.

I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner. This school expects that all activity should be related to a professional use.

I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business. It is my responsibility to ensure that I do not store any inappropriate material on these devices in school. I also understand my responsibilities regarding the use of photographs and videos and how to store these.

I understand that school information systems may not be used for private purposes without specific permission from the head teacher.

I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.

I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.

I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely. I understand that images of children from school cannot be stored on laptops.

I will respect copyright and intellectual property rights.

I will report any incidents of concern regarding children's safety to the Headteacher.

I will ensure that electronic communications with pupils and parents including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted. I fully understand my professional responsibilities, if I chose to use Social Networking Sites.

I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for ICT.

Signed:_____ Date: _____

GREAT MEOLS PRIMARY SCHOOL

Appendix 2

Name: .

POLICY ON THE USE OF SOCIAL NETWORKING WEBSITES

The purpose of the policy is to provide clarity to all school staff on the use of any social networking website, for example Facebook, MySpace, blogs, microblogs such as Twitter, chatrooms, forums, podcasts, open access online encyclopaedias such as Wikipedia, social bookmarking sites such as del.icio.us and content sharing sites such as flickr and YouTube. This is not an exhaustive list, but the principles set out in this policy must be followed irrespective of the electronic medium.

Any member of staff can have an account on a social networking web site. However, it is the responsibility of the individual to ensure that anything placed on the social networking site is appropriate and meets the standards expected of professional teachers and school support staff.

Staff members are strongly advised to ensure that they review privacy levels of their social networking websites to ensure they are 'restricted', and to opt out of public listings to protect their own privacy. This does not negate responsibility for the requirements below.

The policy relates to contact with any young person under 19 years of age, any 'looked after child' under the age of 21 years of age, and any young person with special educational needs under the age of 24 years of age. ***NB School employees who have their own social networking site may have contact with relatives or family friends but all the requirements below would still apply.***

All school staff **must:**

- Demonstrate honesty and integrity, and uphold public trust and confidence in respect of anything placed on social networking web sites.
- Ensure that any content shared on any social networking web site, at any time, would be deemed as appropriate, i.e. staff are personally responsible for ensuring that any privacy settings meet this requirement.
- Ensure appropriate language is used at all times, for any comments placed on social networking sites.
- Ensure that any comments and/or images, at any time, could not be deemed as defamatory or in breach of any relevant legislation.
- Decline 'friend requests' from pupils and ex pupils they receive in their personal social media accounts.

All school staff **must not:**

- Have contact with current/ex pupils, or other children or young people where there is a relationship developed as part of their 'professional' role, e.g. music tutor, on any social networking website.
- Use social networking sites as a forum to make derogatory comments which could bring the school into disrepute, including making comments about pupils, parents, other staff members, the senior leadership team, governors, local authority or the wider community.
- Publish photographs, videos or any other types of image of pupils and their families.
- Use personal communication mediums, e.g. email, mobile phone for contact with pupils.

I have read the policy on the use of social networking websites and understand that any breaches of this policy could result in disciplinary action and may result in dismissal.

Signed	**Date**

This document has been developed and consulted on with Wirral Professional Teachers' Associations and Trade Unions

ASCL Association of School and College Leaders · ATL the education union · NAHT The Association for All School Leaders · NASUWT The Teachers' Union · NUT

Appendix 3

Consent for Video Conferencing Projects

Dear parents/carers,

As part of our curriculum project on _____, the children will be using video-conferencing to communicate with _____ _____. This is an exciting opportunity for your children. We also aim to teach children who to use video conferencing facilities safely.

For your child to take part in this project we need your permission.

Permission for children to participate in video conferencing projects		
Why is permission being sought?	**What are the school's responsibilities?**	
• To help our children interact with different schools/settings using video conferencing facilities.	• To ensure that children only use video conferencing technology when they are supervised by a member of staff. • To ensure that all video conferencing software is password protected. • To ensure that we teach children how to use webcams and other technology safely and appropriately.	
I give permission for my child _____ to participate in the school's video conferencing project.		
	Signature	**Name**

Please complete, sign and return to the School Office.

Kind regards,

Pip Joyce
Headteacher

Appendix 4

Consent for children to be photographed or filmed in school

Why is permission being sought?	
We use photography and video throughout the curriculum. Children may use it to film a piece of drama or a gymnastic routine or take photographs for art etc. We also use photographs to celebrate achievements in school.	
What are the school's responsibilities?	
To ensure that all photographs / videos are appropriate and related to educational purposes. To ensure that all photographs and videos are stored securely on password protected computers. Not to pass any photographs or videos on to any third party without parental permission. To ensure that children's names are not printed next to photographs published online.	
Pupil:	***Year:***
I give permission for my child to be photographed or recorded as part of school activities and for those images to be used for displays in school and on the school website. I agree that my son / daughter's work may be electronically published.	
Signed:	***Date:***
Request permission to take photographs and videos	
I request permission to take photographs and video recordings of my child at authorised school events and confirm these are for my personal use only.	
Signed:	***Date:***
Please print name:	

Please complete, sign and return to the School Office

Appendix 5

Use of Mobile Phones Policy

As part of our safeguarding commitments and e-safety policies, Oak Trees MAT has adopted the following policy regarding the use of mobile phones at school.

The strategies outlined in this policy are designed to ensure that the following does not occur;

- Use of mobile phones to take unauthorised photographs, videos or sound recordings of children.
- Mobile phones being used during working hours by staff.
- Mobile phones being used by visitors in areas of learning.

Children and Mobile Phones

- Children are not allowed to bring mobile phones to school.
- If a mobile phone is brought to school by mistake it must be handed into the school office and collected at the end of the day.
- On rare occasions a child may need to have a mobile phone to assist with special circumstances in attending school (i.e. travelling on the train), the phone should be named and kept in the school office until home time. Walking to school without a parent is not considered special circumstances.
- If a child is found with a mobile phone in school, it will be confiscated and held in the school office until collected by a responsible adult.

Staff and Mobile Phones

- Staff are not allowed to use mobile phones during working hours and they must be turned off.
- Mobile phones can be used during lunch hours, during breaks or outside working hours. These should not be used in the vicinity of children. We suggest that you use mobile phones in unoccupied classrooms, office areas, staff room or the PPA room.
- Staff can use mobile phones for contacting the school office on work related calls. School may provide a work based mobile phone. These should be not be used in close proximity of children.
- We advise staff to call parents on the school phones or school mobile phone and not use their personal phones.
- Staff are not allowed to give parents their personal mobile phone numbers. All communication with parents should be through the school office e-mail system, professional meetings or using the school phone system.
- On residential trips, staff can use mobile phones outside direct hours of supervision, as long as it does not compromise the safety of the children.
- Personal mobile phones cannot be used to take photographs, videos or recordings in school. This includes school trips and residential activities.
- Educational partners will be informed of these policies and asked to follow these guidelines.

These guidelines apply to all staff and students on trainee placements.

Parents and Other Visitors using Mobile Phones

- Parents and other visitors are not allowed to use their mobile phones in school.
- If parents do need to make a call or send a message, they will be asked to step outside the school premises to make the call.
- Parents and visitors will be allowed to take photographs and videos on their phones at **authorised events** as long as they have completed the appropriate permission form.

We ask any parents and visitors not to take any offence if a member of staff requests them to stop using their mobile phone.

Appendix 6

Dear Parent/Guardian,

INTERNET AND ONLINE COMMUNICATION

Oak Trees MAT continually improve its computer facilities, making it possible for pupils to access the Internet, using current devices, to enhance their learning and fulfil elements of the new National Curriculum. This enables pupils to explore thousands of libraries and databases throughout the world, communicate and collaborate on projects and work on interactive educational sites. When appropriate, the children are given individual logins to educational sites such as My Maths and Purple Mash. These sites do not store any information or photographs about your child but we encourage the children to keep their login details private.

Our aim is to use the Internet as an educational resource, and children will be taught to use online technologies sensibly and responsibly. Educational sites such as RM Easimaths and Bug Club have built-in safeguards to prevent children gaining access to unsuitable material, but the wider Internet may contain unsuitable websites.

In order to reduce the possibility of pupils gaining access to these sites, we have set the following procedures in place:-

- Our broadband is provided by Exa Networks who use Surf Protect (Becta approved) as a filtering service designed to deny access to inappropriate images and sites including chat rooms.
- Pupils in Key Stage 2 will be allowed to browse the Internet. Pupils in Foundation 2 and Key Stage 1 will be allowed to work on sites pre-selected by their teacher or other authorised adults.
- Pupils will be supervised at all times by a member of staff or other authorised adult who will provide guidance to pupils as they make use of online technologies to further their curriculum studies.
- Staff will inform all pupils about their rights and responsibilities as users of the Internet prior to gaining access.
- As far as possible, pupils will be directed to information sites that have been reviewed and evaluated beforehand. If pupils move beyond those sites, the supervising adult will give guidance about the suitability and relevance of the site.

Our intention is to use the Internet to further the Academy's educational aims and enhance the curriculum, whilst at the same time safeguarding pupils from any potentially inappropriate or harmful elements. With this in mind I would ask for your assistance in conveying the standards that should be followed by your child when using the Internet. In addition to speaking with your child about these matters, would you please complete the attached form with your child and return it to school.

Your co-operation in this matter would be much appreciated.

Yours sincerely,

Pip Joyce
Headteacher

Appendix 7

E-Safety Rules Consent Form

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum.

Both pupils and their parents/guardians are asked to sign to show that the e-safety rules have been understood and agreed.

Our E-Safety Policy is available from the school office and is published on the school's website.

Pupil:	***Year:***

Pupil's Agreement

- I understand the school e-safety rules.
- I will use the computer, network, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed:	***Date:***

Parent / Guardian's Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:	***Date:***

Please print name:

Please complete, sign and return to the School Office

Appendix 8

E-Safety Rules
for
Key Stage 1

Think Then Click!

E-Safety Rules for Key Stage 1

These rules help us to stay safe on the Internet

- **We only use the Internet when an adult is with us.**
- **We can click on the buttons or links when we know what they do.**
- **We can search the Internet with an adult.**
- **We always ask if we get lost on the Internet.**
- **We can communicate online with an adult's help.**
- **We are polite and friendly when communicating online.**
- **We know who to tell if we feel uncomfortable when online.**
- **We only give out personal information online when we are with an adult.**

Appendix 9

E-Safety Rules
for
Key Stage 2

Think Then Click!

E-Safety Rules for Key Stage 2

These rules help us to stay safe on the Internet

- We ask permission before using the Internet.
- We only use websites that an adult has chosen or approved.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we are not sure about.
- We only communicate with people an adult has approved.
- We communicate online in a friendly and polite manner.
- We recognise and know how to report unacceptable behaviour.
- We never give out personal information or passwords.
- We never arrange to meet anyone that we don't know in the offline World.
- We do not open messages from people we don't know.
- We do not use Internet chat rooms.
- We do not use mobile phones in school.
- We know who to contact if we have concerns when online.