E-Safety Policy

E-Safety Policy

1 Our Vision for E-Safety

1.1 ICT is an increasingly essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. We recognise that all schools need to build on the use of these technologies in order to arm young people with the appropriate skills to access life-long learning and employment.

1.2 ICT now covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. The internet technologies children and young people are using include:

- Website
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting/Live Streaming
- Music Downloading
- Gaming – Augmented Reality/Virtual Reality/ Voice chat
- Mobile phone Apps - Ephemeral or expiring content
- Mobile/ Smart phones/Smart Watches and tablets with text, video and/ or web functionality including Geolocation
- Smart Televisions
- Other mobile devices and games consoles with web functionality

1.3 At Oakfield School we understand our responsibility to educate our pupils on ‘online’ issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the classroom environment. We believe it is essential for E-Safety guidance to be given to the pupils on a regular and meaningful basis.

1.4 Pupils are always reminded that reporting an online issue is very important in keeping yourself safe.

- Always tell a staff member if an issue has occurred they will support you and help with this matter. (Staff will follow school’s protocols relating to the issue)
- If pupils are at home, you must tell your parent/carers or a responsible adult
- Pupils are reminded to never delete information sent to them.

1.5 E-Safety is embedded within our curriculum and we continually look for new opportunities to promote safe use of the online world.

1.6 Our vision is that pupils have a diverse, balanced and relevant approach to the use of technology, in an environment where security is balanced appropriately with the need to learn effectively. We aim to ensure that our children are equipped with the skills and knowledge to use technology appropriately and responsibly, that they understand the risks associated with this activity and are able to deal with these both in and out of school.

1.7 Oakfield School's E-Safety Policy has been written to ensure safety measures are in place to protect both students and staff working with ICT equipment and related technologies. The policy is to assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own and student's standards and practice. Our responsibility is to set high expectations of our students using communication technologies and to maintain a consistent approach to E-Safety by knowing the content of the policy and the procedures adopted and developed by the school.

2 Scope of Policy

2.1 This policy applies to the whole school community including Oakfield's Senior Leadership Team, all staff employed directly or indirectly by the school.

2.2 Oakfield's Senior Leadership Team will ensure that any relevant or new legislation that may impact upon the provision for E-safety within school will be reflected within this policy.

2.3 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. This is pertinent to incidents of online bullying, or other online related incidents covered by this policy, which may take place out of school, potentially at commissioned provision, but is linked to membership of the school.

2.4 The school will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate online behaviour that takes place out of school.

2.5 Use of ICT equipment and data in any format should be handled in line with the school's Data Protection Policy, and GDPR regulations.

3 Review & Ownership

3.1 This E-Safety Policy:

- has been endorsed and agreed by the Senior Leadership Team and approved by the Governors.
- will be reviewed annually or when any significant changes occur with regards to the technologies in use within the school.

3.2 The school has appointed the Deputy Headteacher and Child Protection Coordinators to take the lead responsibility for E-Safety.

3.3 Amendments to the school E-safety policy will be discussed in detail with all members of teaching staff and training will be given which will link to relevant and current guidance and legislation.

4 Responsibilities

4.1 We believe that E-Safety is the responsibility of the whole school community, and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following list of responsibilities shows how each member of the community will contribute to the school vision.

4.2 **Senior Leadership Team (SLT):**

4.2.1 The Headteacher is ultimately responsible for safeguarding provision (including E-Safety) for all members of the school community, with day-to-day responsibility for E-safety delegated to the Deputy Headteacher and Child Protection Officer.

4.2.2 The Headteacher and SLT are responsible for ensuring that the Child Protection Coordinator and other relevant staff receive effective and up to date training to enable them to carry out their E-safety roles and to train other colleagues when necessary.

4.2.3 The SLT will receive updates from the Child Protection Officer as appropriate.

4.2.4 The Headteacher and SLT will ensure that procedures are rigorously followed in the event of all E-Safety incidents.

4.2.5 The Headteacher and SLT will receive timely, regular and routine updates and reports on all E-Safety incidents.

4.2.6 The team will ensure that E-safety education is appropriately embedded across the whole curriculum.

4.2.7 It is the responsibility of all staff including the SLT to ensure that all use of ICT equipment and data in any format, should be handled in line with the school's Data Protection Policy, and GDPR regulations.

4.3 **The Deputy Headteacher and Chid Protection Coordinators:**

4.3.1 Will promote an awareness and commitment to E-Safety throughout the school.

4.3.2 Will be the first point of contact in school on all E-Safety matters.

4.3.3 Will take day-to-day responsibility for E-Safety within school and to have a leading role in establishing and reviewing the school E-Safety policies and procedures.

4.3.4 Have regular contact with other E-safety committees, e.g. the local authority, Local Safeguarding Children Partnership (along with the Child Protection Coordinators).

4.3.5 Will communicate regularly with the schools RM ICT technician, the designated E-Safety representative for the Management Committee and the SLT.

4.3.6 Will create and maintain E-Safety policies and procedures, reporting to the Governors at least annually.

4.3.7 Will ensure that E-Safety is promoted to parents and carers.

4.3.8 Liaise with the local authority, the Local Safeguarding Children Partnership and other relevant agencies as appropriate.

4.3.9 Monitor and report on E-safety issues to the SLT as appropriate.

4.3.10 Understand the issues surrounding the sharing of personal or sensitive information.

4.3.11 It is the responsibility of all staff including the SLT to ensure that all use of ICT equipment and data in any format, should be handled in line with the school's Data Protection Policy, and GDPR regulations.

4.4 **Teachers and Support Staff**

4.4.1 Read, understand and actively promote the school's E-safety policies and guidance.

4.4.2 Read, understand and adhere to the school staff Acceptable Use Agreement.

4.4.3 Ensure that any E-safety incidents are reported under appropriate escalation routes.

4.4.4 Develop and maintain an awareness of current E-safety issues and guidance.

4.4.5 Model safe and responsible behaviours in their own use of technology.

4.4.6 Ensure that any digital communications with pupils should be on a professional level and only through school based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones, social networking, etc.

4.4.7 Embed E-safety messages in learning activities across all areas of the curriculum.

4.4.8 Supervise and guide pupils carefully when engaged in learning activities involving technology.

4.4.9 Ensure that pupils are fully aware of research skills and methods.

4.4.10 Be aware of E-safety issues related to the use of mobile phones, cameras and handheld devices.

4.4.11 Understand and be aware of incident-reporting mechanisms that exist within the school.

4.4.12 Maintain a professional level of conduct in personal use of technology at all times.

4.4.13 It is the responsibility of all staff to ensure that all use of ICT equipment and data in any format, should be handled in line with the school's Data Protection Policy, and GDPR regulations.

4.5 **All Staff & Commissioned Partners, are required to:**

4.5.1 Be aware of the school's E-Safety Policy and guidance.

4.5.2 Read, understand and adhere to the school staff Acceptable Use Agreement.

4.5.3 Report any E-safety related issues that come to their attention to the Child Protection Coordinators.

4.5.4 Develop and maintain an awareness of current E-safety issues, legislation and guidance relevant to their work.

4.5.5 Maintain a professional level of conduct in the use of technology at all times.

4.5.6 Support the school in providing a safe technical infrastructure to support learning and teaching.

4.5.7 Ensure that pupil access to the school network is only through an authorised, restricted mechanism.

4.5.8 It is the responsibility of all staff to ensure that all use of ICT equipment and data in any format, should be handled in line with the school's Data Protection Policy, and GDPR regulations.

4.6 **Pupils, are required to:**

4.6.1 Understand and adhere to the Acceptable Use Policy.

4.6.2 Pupils who are unable to understand the Acceptable Use Policy may require a parent/ carer to sign on their behalf.

4.6.3 Help and support the school in the creation of E-safety policies and practices and to adhere to any policies and practices the school creates.

4.6.4 Where appropriate pupils will be expected to understand school policies on the use of mobile phones, digital cameras and handheld devices.

4.6.5 Know and understand school rules relating to bullying and online bullying.

4.6.6 Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.

4.6.7 Understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to.

4.6.8 Understand the importance of reporting abuse, misuse or access to inappropriate materials and to understand the incident-reporting mechanisms that exists within school.

4.6.9 Discuss E-Safety issues with family and friends in an open and honest way.

4.6.10 E-Safety lessons students can understand and contribute to the effectiveness of the E-safety processes.

4.6.11 Parents and Pupils have been informed of the schools Data Protection Policy, and the impact of GDPR regulations on data handling and sharing.

4.7 **Parents/Carers, are required to:**

4.7.1 Help and support the school in promoting E-Safety.

4.7.2 Read, understand and promote the school pupil Acceptable Use Policy with their children.

4.7.3 Take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home.

4.7.4 Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

4.7.5 Discuss E-safety concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology.

4.7.6 Model safe and responsible behaviours in their own use of technology.

4.7.7 Consult with the school if they have any concerns about their children's use of technology.

4.7.8 Sign the photography permission form stating where photographs are to be published upon admission.

4.7.9 Parents/carers and pupils have been informed of the school's Data Protection Policy, and the impact of GDPR regulations on data handling and sharing.

5 Managing Digital Content

5.1 Before photographs of pupils can be published, permission must be granted formally and agreed and signed by parents or guardians. All staff should be aware of the process involved with publishing images over different mechanisms.

5.2 Parents and carers may withdraw permission, in writing, at any time. A procedure exists for permission to be removed retrospectively.

5.3 The school will remind pupils of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.

5.4 Pupils and staff will only use school equipment to create digital images, video and sound.

5.5 Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking.

5.6 When searching for images, video or sound clips, staff will be taught about copyright and acknowledging ownership.

5.7 It is the responsibility of all staff including the Senior Leadership Team to ensure that all use of ICT equipment and data in any format, should be handled in line with the school's Data Protection Policy, and GDPR regulations. All staff are required to sign that they have attended and understood GDPR training, and that any personal or school devices are compliant with GDPR.

6 Storage of Images

6.1 Any images, videos or sound clips of pupils must be stored on the school network and never transferred to personally-owned equipment.

6.2 Individual staff members have the responsibility of deleting the images when they are no longer required, or when a pupil has left the school. This instruction will come from a member of the SLT once a procedure and agreement has been decided.

7 Teaching & Learning

7.1 We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings. We recognise that three main areas of E-Safety risk as highlighted by Ofsted are:

7.1.1 Content – Children and our communities need to be taught that not all content is appropriate or from a reliable source.

7.1.2 Contact – Children and stakeholders need to be made aware that digital technologies may be used as a vehicle for grooming, online bullying and identity theft, and understand how to deal with these risks if they occur.

7.1.3 Conduct – Children and parents need to be aware that their personal behaviour on line and their electronic identity can increase the likelihood of, or cause harm to themselves and others. Key risk areas being disclosure of personal information, issues around sexting, privacy issues and copyright issues.

8 In order to minimize these risk to our pupils at the school, we will:

8.1 Discuss, remind or raise relevant E-safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others.

8.2 Deliver enrichment classes relating to personal safety which can be targeted to vulnerable individuals or groups.

8.3 Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.

8.4 Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.

8.5 Staff will model safe and responsible behaviour in their own use of technology during lessons.

8.6 Pupils will be taught about the impact of bullying and online bullying and know how to seek help if they are affected by any form of online bullying.

8.7 Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent / carer, teacher / trusted staff member, or an organisation such as Childline / CEOP (Child Exploitation & Online Protection).

8.8 In the event of a crisis, such as the Covid pandemic, some pupils will be expected to work remotely. Digital work is sent via Microsoft Teams and all efforts have been made to create a safe environment to complete this work. Teams is set up in a way that inappropriate material cannot be sent to others including pupils and staff and the chat function between pupils has been disabled.

9 Staff Training & Awareness

9.1 Our staff will receive regular information and training on E-Safety issues in the form of regular and routine updates and when appropriate.

9.2 As part of the induction process all new staff will receive information and guidance on the E-Safety Policy and the school's Acceptable Use Policy.

9.3 All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community.

9.4 All staff will be required to incorporate E-Safety activities and awareness within their curriculum areas.

9.5 Safeguarding Level 1.

9.6 CEOP (Child Exploitation and Online Protection) Training.

9.7 GDPR Training.

10 Managing ICT Systems & Access (this will be managed by Oakfield School and RM)

10.1 The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.

10.2 Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.

10.3 Servers, workstations and other hardware and software will be kept updated as appropriate.

10.4 Virus protection is installed on all appropriate hardware, and will be kept active and up to date.

10.5 Members of staff will access the network using an individual username and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the network through their username and password. They will abide by the school Acceptable Use Policy, amended in line with GDPR, at all times.

10.6 All pupils, when appropriate, will have a unique username and password for access to ICT systems.

11 Passwords

11.1 A secure and robust username and password convention exists for all system access.

11.2 Staff should be prompted to change their passwords at prearranged intervals or at any time that they feel their password may have been compromised.

11.3 Staff should change their passwords whenever there is any indication of possible system or password compromise.

11.4 Pupils passwords will be managed by the appropriate member of support / teaching staff and changed when is deemed appropriate. Pupil passwords will be unique for all.

11.5 All staff have a responsibility for the security of their username and password. Staff must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. Staff are expected to comply with the following password rules:

- Do not write down system passwords.
- Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed as soon as possible.
- Always use your own personal passwords to access computer based services, never share these with other users.
- Make sure you enter your personal passwords each time persons' login to your system. Do not include passwords in any automated logon procedures.
- Never save system-based usernames and passwords within an internet browser

12 New Technologies

12.1 As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an E-Safety point of view. We will regularly amend the E-Safety Policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an E-Safety risk.

12.2 The school will audit ICT equipment usage to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate.

12.3 The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.

13 Mobiles Phone, Smart Phones & Smart Watches

13.1 Pupils are advised not to bring mobile phones and nor other devices to school, however if they do bring them in, there is an expectation that they will manage the use of their mobile phone appropriately and not access social network / media whilst at school. If inappropriate use is

deemed, then pupils will be challenged and this could lead to the phone being confiscated.

13.2 Mobile Phones /other devices are not permitted for use during lesson times.

13.3 Pupils should not use personal devices such as mobile phones or cameras to take photos or videos of any persons.

13.4 If students fail to use their mobile device appropriately then a member of staff can remove their device.

13.5 Sanctions will be used if this expectation is misused

14 Staff Use of Mobiles Devices

14.1 Staff members are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity. All of the staff have access to either a school mobile phone or main line telephone.

14.2 Staff will use a school phone to contact parents or carers within the hours of the school opening times.

14.3 Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work provided equipment for this purpose.

14.4 Staff are not permitted to use their personal mobile phones or personal devices during working school hours, unless with prior agreement with the Headteacher/Deputy Headteacher and only in cases of emergencies.

14.5 If a member of staff breaches the school policy, then disciplinary action may be taken.

14.6 It is the responsibility of all staff to ensure that all use of ICT equipment and data in any format, should be handled in line with the school's Data Protection Policy, and GDPR regulations. All staff are required to sign that they have attended and understood GDPR training, and that any personal or school devices are compliant with GDPR.

15 Filtering Internet Access

15.1 The school filters and monitors its internet provision appropriate to the age and maturity of pupils. – filtering is externally managed internally with smoothwall and RM (ICT facilities management)

15.2 The school will always be proactive regarding the nature of content which can be viewed through the school's internet provision.

15.3 The school has a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Agreement and by attending the appropriate awareness training.

15.4 If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the E-Safety Coordinator. All incidents should be documented and reported to RM to be blocked.

15.5 If users discover a website with potentially illegal content, this should be reported immediately to the Deputy Head and Child Protection Coordinators who will liaise with RM. All incidents will be logged and chronologically recorded; the school will report such incidents to appropriate agencies including the filtering provider, the local authority or CEOP.

15.6 The school will regularly review incidents through the Child Protection Coordinators' meeting. All concerns can be highlighted to external contractors RM in the contractual discussions.

15.7 Pupils will be taught to assess content as their internet usage skills develop.

15.8 Pupils will use age-appropriate tools to research internet content.

15.9 The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

15.10 The smoothwall also sends daily reports to the E-Safety officers to alert them to any suspicious usage

16 Internet Access Authorisations

16.1 All parents will be required to sign a home-school agreement prior to their children being granted internet access in school. This consent is embedded into a robust admission process whereby appropriate access, internet usage and E-safety is discussed and agreed prior to admission.

16.2 Parents will be asked to read the school Acceptable Use Agreement for pupil access and discuss it with their children, when and where it is deemed appropriate.

16.3 All pupils will have the appropriate awareness training through E-safety briefing through the admission process and through lessons. All pupils are expected to sign the pupils Acceptable Use Agreement.

16.4 Parents will be informed that pupils will be provided with supervised internet access appropriate to their age and ability.

16.5 The school will maintain a current record of all staff and pupils who have been granted access to the school's internet provision.

16.6 All pupils will be supervised and monitored during their use of the internet. Pupils will be frequently reminded of internet safety issues and safe usage.

17 Email

17.1 Staff members are required to comply with the following:

- Staff should only use approved email accounts allocated to them by the school and should be aware that use of the school email system is monitored and checked.
- Staff should not use personal email accounts during school hours or for professional purposes, especially to exchange any school-related information or documents.
- Access, in school, to external personal email accounts may be blocked.
- The school gives all staff their own email account to use for all school business as a work-based tool. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- Staff members are responsible for keeping their password secure.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- Irrespective of how staff access their school email (from home or within school), school policies still apply.
- All emails that are no longer required or of any value should be deleted.
- Staff should check email accounts regularly for new correspondence.
- All email and email attachments will be scanned for malicious content.
- Staff should never open attachments from an untrusted source.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.

- Any inappropriate use of the school email system or receipt of any inappropriate messages from another user should be reported to the Deputy Head immediately.
- All email users within school should report any inappropriate or offensive emails to the Deputy Head.
- All staff are required to sign that they have attended and understood GDPR training, and that any personal or school devices are compliant with GDPR. Any email sent to outside agencies must be sent from a designated Oakfield School email address, and any shared data must be GDPR compliant, including the encryption of attachments.

18 Use of Social Media

18.1 Staff must not talk about their professional role in any capacity when using personal social media such as Facebook and YouTube or any other online publishing websites.

18.2 Staff and pupils are asked to report any incidents of online bullying to the school.

18.3 Staff will raise any concerns about pupil use of social media sites with parents/carers this includes the use of any sites that are not age appropriate.

18.4 All staff will receive training on the risks associated with the use of social media either through staff meetings or via the induction process for new starters. Safe and professional behaviour is outlined in the Acceptable Use Policy.

18.5 Staff must not use social media tools to communicate with current or former pupils.

18.6 Staff will not use any social media tools to communicate with parents.

18.7 Procedures for dealing with online bullying incidents of staff or pupils involving social media are outlined in the school Anti-Bullying policy.

18.8 Staff members are advised to set and maintain profiles on such sites to maximum privacy.

19 Use Memory Sticks

19.1 Staff are permitted to use non – encrypted USB memory sticks for use of non-confidential information i.e. lesson planning, activity planning.

19.2 Staff are NOT permitted to use non – encrypted USB memory stick for sensitive information.

19.3 Sensitive information must always be agreed with the Headteacher, Deputy Headteacher or the Head of Care before any downloading of details occurs.

19.4 Staff are not permitted to download any confidential material without prior agreement with the Headteacher, Deputy Headteacher or Head of Care.

19.5 Staff must always conform to the General Data Protection (GDPR) 2018 and the school's Data Protection Policy.

20 Electronic Bullying & Harassment

20.1 This E-Safety Policy recognises the additional dangers of online bullying. All staff and pupils should be aware that any misuse of ICT to bully or harass others will be dealt with under the school Anti Bullying policy, and are reminded that:

20.2 'Bullying is behaviour by an individual or group, repeated over time, which intentionally hurts another individual or a group physically or emotionally. Bullying can take many forms (for instance, cyber-bullying via text messages or the internet), and is often motivated by prejudice against particular groups (for example on grounds of race, religion, gender, sexual orientation, or because a child is adopted or has caring responsibilities). It might be motivated by actual difference between children, or perceived differences. Stopping violence and ensuring immediate physical safety is obviously a first priority but emotional bullying can be more damaging than physical.'

20.3 All staff will have to make their own judgements about each specific case.

21 Online Sexual Harassment

21.1 Sexual Harassment is likely to: violate a child's dignity, make them feel intimidated, degraded or humiliated and/or create a hostile, offensive or sexualised environment.

21.2 Online sexual harassment, which might include: non – consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as Sexting), inappropriate sexual comments on social media, exploitation: coercions and threats.

21.3 Any report of online sexual harassment will be taken seriously, and the Police and Children's Social Care may be notified.

21.4 Our school follows and adheres to the national guidance - UKCCIS Sexting in schools and Colleges: Responding to incidents and safeguarding young people 2016.

22 Sexing & School Protocols in dealing with incidents

22.1 'Sexting' is one of a number of 'risk-taking' behaviours associated with the use of digital devices, social media or the internet. It is accepted that young people experiment and challenge boundaries and therefore the risks associated with 'online activity' can never be completely eliminated. However, Oakfield School takes a pro-active approach in its ICT and Enrichment programmes to help students to understand, assess, manage and avoid the risks associated with 'online activity'. The school recognises its duty of care to its young people who do find themselves involved in such activity as well as its responsibility to report such behaviours where legal or safeguarding boundaries are crossed.

22.2 There are a number of definitions of 'sexting' but for the purposes of this policy sexting is simply defined as:

- Images or videos generated by children under the age of 18, or of children under the age of 18 that are of a sexual nature or are indecent.
- These images are shared between young people and/or adults via a mobile phone, handheld device, computer, 'tablet' or website with people they may not even know.

22.3 The Child Protection Coordinators / Deputy Child Protection Coordinator and the Deputy Headteacher need to be informed of any 'sexting' incidents. The range of contributory factors in each case also needs to be considered in order to determine an appropriate and proportionate response. All staff are expected to be aware of this policy.

22.4 **Step 1 – Disclosure by a pupil**

22.4.1 'Sexting' disclosures should follow the normal safeguarding practices and protocols (refer to the schools Child Protection Policy).

22.4.2 A pupil is likely to be very distressed especially if the image has been circulated widely and if they don't know who has shared it, seen it or where it has ended up.

22.4.3 The Emotional Wellbeing Team will engage and offer support to the pupil affected.

22.4.4 The Child Protection Coordinators / Deputy Child Protection Coordinator will initiate contact with the appropriate services, this may include referral to police or Social Services and the Local Authority. Parents should be informed as soon as possible (police advice permitting).

22.4.5 The following questions will help decide upon the best course of action:

- Is the pupil disclosing about themselves receiving an image, sending an image or sharing an image?
- What sort of image is it? Is it potentially illegal or is it inappropriate?
- Are the school child protection and safeguarding policies and practices being followed?
- How widely has the image been shared and is the device in their possession?
- Is it a school device or a personal device?
- Does the pupil need immediate support and/or protection?
- Are there other pupils involved?
- Do they know where the image has ended up?

22.5 Step 2 – Searching A Device

22.5.1 Please refer to the school's Search, Screening and Confiscation Protocols, which are based on the most current legislation, The 2011 Education Act.

22.5.2 The policy allows for a device to be examined, confiscated and securely stored if there is reason to believe it contains indecent images or extreme pornography. When searching a mobile device, the following conditions should apply:

- The search is conducted either by the Headteacher or a person authorised by them (or Deputy Headteacher or Child Protection Coordinators/ Deputy Child Protection Coordinator).
- A member of the Senior Leadership Team should normally be present.
- The search should normally be conducted by a member of the same gender as the person being searched. However, if the image being searched for is likely to be of a different gender to the person 'in possession' then the device should only be viewed by a member of the same gender as the person whose image it is.
- If any illegal images of a young person are found, then the Child Protection Protocols are immediately initiated.

22.5.3 The Association of Chief Police Officers (ACPO) advise that as a general rule it will almost always be proportionate to refer any incident involving 'aggravated' sharing of images to the Police, whereas purely 'experimental' conduct may proportionately have dealt with without such referral, most particularly if it involves the young person sharing images of themselves.

22.5.4 ‘Experimental conduct’ commonly refers to that shared between two individuals (e.g. girlfriend and boyfriend) with no intention to publish the images further. Coercion is not a feature of such conduct, neither are requests for images sent from one person to multiple other young persons.

22.5.5 Any conduct involving, or possibly involving, the knowledge or participation of adults should always be referred to the police.

22.5.6 If an ‘experimental’ incident is not referred to the Police, the reasons for this should be recorded by the Child Protection Coordinators/ Deputy Child Protection Coordinator. Always put the young person first. Do not search the device if this will cause additional stress to the student/person whose image has been distributed. Instead rely on the description by the young person, secure the advice and contact the Police.

Never:

- Search a mobile device, even in response to an allegation or disclosure, if this is likely to cause additional stress to the pupil **unless** there is clear evidence to suggest not to do so would impede a police inquiry.
- Print out any material for evidence
- Move any material from one storage device to another

Always:

- Staff will immediately Inform Jayne Oakley, Leanne Middleton (Child Protection Co coordinators), Jo Jordan (Deputy Child Protection Coordinator), Leanne Smith (Deputy Head) and or Headteacher, Rachel Davies who will ensure that the Designated Safeguarding Lead is able to take any necessary strategic decisions.
- Record the incident on a Cause for Concern Form.
- Act in accordance with school safeguarding Screening, Search and Confiscation protocols

22.5.7 If there is an indecent image of a child on a website or a social networking site, then the Child Protection Coordinator will report the image to the site hosting it. Under normal circumstances the school would follow the reporting procedures on the respective website; however, in the case of a sexting incident involving a child or young person where it may be felt that they may be at risk of abuse then the team will report the incident directly to CEOP www.ceop.police.uk/ceop-report , so that law enforcement can make an assessment, expedite the case with the relevant provider and ensure that appropriate action is taken to safeguard the child.

22.6 **Step 3 – What to do and not do with the image**

22.6.1 If the image has been shared across a personal mobile device:

Always:

- Confiscate secure the device(s). Close down or switch the device off as soon as possible. This may prevent anyone removing evidence 'remotely'.

Never:

- View the image unless there is a clear reason to do so or view it without a member of the Senior Leadership Team present (this additional person does not need to view the image and certainly should not do so if they are of a different gender to the person whose image has been shared). The viewing of an image should only be done to establish that there has been an incident which requires further action.
- Send, share or save the image anywhere
- Allow pupils to do any of the above

22.6.2 If the image has been shared across a personal mobile device:

Always:

- Block the network to all users and isolate the image.

Never:

- Send or print the image
- Move the material from one place to another
- View the image outside of the protocols in the school's safeguarding and child protection policies and procedures.

22.7 **Step 4 – Who should deal with the incident?**

22.7.1 All staff for information purposes, and completion of relevant paperwork, (Cause for Concern).

22.7.2 All safeguarding/E safety/E security incidents should be reported to the Child Protection Coordinators/ Deputy Child Protection Coordinator and or Deputy Head who will then deal with the incident.

22.7.3 The Child Protection Coordinators will initiate Child Protection Procedures. The Headteacher and or Deputy Head should also always be informed- usually by the Child Protection Coordinators. There may be instances where the image needs to be viewed and this should be done in accordance with protocols.

22.8 Step 5 – Deciding on a response

22.8.1 There may be many reasons why a pupil has engaged in sexting – it may be a romantic/sexual exploration scenario or it may be due to coercion.

22.8.2 It is important to remember that it won't always be appropriate to inform the police; this will depend on the nature of the incident. However, as a school it is important that incidents are consistently recorded. It may also be necessary to assist the young person in removing the image from a website or elsewhere

22.8.3 If indecent images of a pupil / young person are found:

- Act in accordance with the Child Protection Policy/Procedures i.e. inform the Child Protection Coordinators and Deputy Head.
- Store the device securely
- The Child Protection Coordinators/ Deputy Child Protection Coordinator will make a referral if needed.
- The Safeguarding Team will contact the police (if appropriate). Referrals may be made to Social Care or the Multi-Agency Team (MAT) but where a crime may have thought to have taken place the police are the first port of call. Young persons who have engaged in 'experimental sexting' which is contained between two persons will be referred to MAT for support and guidance. Those who are felt to be victims of 'sexting' will also be referred to MAT at a point where the police feel that this will not impede an investigation.
- Inform parents and/or carers about the incident and how it is being managed.

22.9 Step 6 – Containment and Prevention

22.9.1 The pupil involved in 'sexting' may be left feeling sensitive and vulnerable for some time. They will require monitoring by and support from the Emotional Wellbeing Team and or Keyworker.

22.9.2 Where cases of 'sexting' become widespread or there is thought to be the possibility of contagion, then the school will reinforce the need for safer 'online' behaviour using a variety of resources.

22.9.3 Other staff may need to be informed of incidents and should be prepared to act if the issue is continued or referred to by other pupils. The school, its pupils and parents should be on high alert, challenging behaviour and ensuring that the victim is well cared for and protected. The pupil's parents should usually be told what has happened so that they can keep a watchful eye over the young person, especially when they are online at home.

22.9.4 Creating a supportive environment for pupil in relation to the incident is very important.

22.9.5 Preventative educational programmes on sexting can be found on CEOP's advice-giving website www.thinkunknow.co.uk

23 Dealing with Incidents

23.1 All E-Safety incidents at the school are logged within the E-Safety Incident Log, which is located in the Administration Office for staff to disclose concerns. They are also required to inform the Deputy Head and the Child Protection Coordinator, then procedures will be initiated to deal with the incident.

23.2 An important element of E-safeguarding is the ability to identify and deal with incidents of concern including the confidentiality of information. All staff/volunteers, children and young people have a responsibility to report e-safety or e-security incidents so that they may be dealt with effectively and in a timely manner in order to minimise any impact.

23.3 Oakfield School have an incident reporting procedure and record reported incidents in an 'Incident Log'.

23.4 The Incident Log and the school's policy should be reviewed annually by the Governing Body.

23.5 When incident have been reported, the Child Protection Coordinators/ Deputy Child Protection Coordinator and the Deputy Head will decide what action will be taken; this will be documented on the Incident Log /outcome.

23.6 Any suspected illegal materials or activity must be brought to the immediate attention of the Child Protection Coordinators – Jayne Oakley/Leanne Middleton and Deputy Head, Leanne Smith, who will refer this to appropriate external agencies such as Children's Social Care, Local Authority Designated Officer, Dan Horn, Prevent Coordinator, Karen Windross, Police and or CEOP.

23.7 Examples of illegal Offences are:

- Accessing Child Abuse Images
- Accessing Criminally Obscene Content
- Inciting Racial Hatred
- Accessing Sexual Child Abuse Images and Content.

23.8 Staff should never under any circumstances investigate, interfere or share evidence of these activities as they may themselves be committing an illegal offence in doing so. Further information is available from www.iwf.org.uk

23.9 Inappropriate Use. Staff and pupils at Oakfield School are likely to deal with “accidental” access to inappropriate materials and content or inappropriate use.

23.10 Examples of these and the actions and sanctions to apply are as follows:

- Accidental access to inappropriate materials - recommendation is to minimise the applications, immediately turn off the monitor. Pupil should tell a member of staff. Staff will enter the details on the incident log and inform Child Protection Coordinators, Deputy Head and RM.
- Using other people’s logins, accounts or passwords
- Deliberate searching for inappropriate materials
- Bringing inappropriate electronic media into school
- Inappropriate use of chat and forum.

23.11 Recommendation for each of the above is to inform Child Protection Coordinators, reiterate and raise E Safety issues with individuals or class and for more serious or persistent offences consider further action, meeting with parents/carers, Child Protection Coordinators to investigate further.

24 Evaluating the Impact of this E-Safety Policy

24.1 The Senior Leadership Team will regularly and routinely monitor and evaluate the impact of this policy by monitoring the number and range of E-Safety incidents in the school, regularly testing and checking on pupil’s awareness of E-Safety issues and looking for patterns and trends in practice.

24.2 Policy Statement Disclaimer:

- Oakfield School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a computer.
- Neither Oakfield School nor Hull City Council can accept liability for the material accessed, stored or distributed or any consequences resulting from Internet use.

- Oakfield School should audit digital technological use to establish if the E–Safety Policy is adequate and that the implementation of the E–Safety Policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

25 Monitoring & Review

25.1 This policy will be monitored and reviewed annually. It has been approved by the Chair of Governing Body, Headteacher, Deputy Headteacher and Child Protection Officer.

25.2 The new review will be January 2023 unless guidance changes then this policy will be amended according to statutory/national guidance.

Information on Support/Guidance

www.thinkuknow.co.uk

www.disrepectingnobody.co.uk

www.saferinternet.org.uk

www.internetmatters.org

www.childnet.com/cyberbullying-guidance

www.pshe.association.org.uk

http://educateagainsthate.com/

Searching, Screening and Confiscation – January 2018

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/554415/searching_screening_confiscation_advice_Sept_2018.pdf

Keeping Safe in Education – September 2020

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/550511/Keeping_children_safe_in_education.pdf

The Prevent Duty – June 2015

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/439598/prevent-duty-departmental-advice-v6.pdf

Hull Safeguarding Children Partnership

http://hullscb.proceduresonline.com/

National Guidance UKCCI - Sexting in School and Colleges 2016

The law and statutory guidance

Malicious Communication Act 1988
This Act covers the sending of grossly offensive or threatening letters, electronic communications or any other form of message with the intention of causing harm, distress or anxiety.

Children Act 1989
This Act describes the paramount nature of children's welfare and the duty care agencies and organisations have to protect them.

Computer Misuse Act 1990
The Computer Misuse Act makes it an offence to access computer material without permission to:

• look at someone's files
• access someone's files with the intent to commit a criminal offence

Communications Act 2003
Section 127 of the Act makes it an offence to send anything that is indecent or grossly offensive.

Digital Economy Act 2017
The Digital Economy Act provides important protection for citizens from spam email and nuisance calls and protects under 18s from accidental exposure to online pornography.

IWF – Internet watch foundation – **last update to articles January 2021**

https://www.iwf.org.uk/

SWGFL

https://swgfl.org.uk/resources/safe-remote-learning/

H.S.C.P

https://hullscb.proceduresonline.com/chapters/p_esafety_abuse_dig_media.html

https://learning.nspcc.org.uk/research-resources/schools/e-safety-for-schools

See **Safety in a Digital World: Guidance and Acceptable Use Policies Template**

See **UK Safer Internet website** and **CEOP, thinkUknow website**

Childnet Advice on Sexting

Coram Children's legal centre – Law Stuff is run by Coram Children's Legal Centre and gives free legal information to young people on a range of different issues. See Children's rights in the digital world in particular.

Child Safety Online: A Practical Guide for Parents and Carers whose Children are Using Social Media

Staying Safe Online – Guide for Children and Young People (Hull Safeguarding Children's Partnership)

Social Media as a Catalyst and Trigger for Youth Violence (Catch 22)

Behaviour that is illegal if committed offline is also illegal if committed online. It is recommended that legal advice is sought in the event of an online issue or situation. There are a number of pieces of legislation that may apply including:

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.

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 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

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 on one occasion (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 practitioners, youth workers staff fall in this category of trust.) Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Serious Crime Act 2015

The Act introduces a new offence of sexual communication with a child. This would criminalise an adult who communicates with a child for the purpose of obtaining sexual gratification, where the communication is sexual or if it is intended to elicit from the child a communication which is sexual and the adult reasonably believes the child to be under 16.

Guidance on teaching online safety

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf

https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Articles on web sites for information

https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/online-safety-policy

Online Safety for children and young people with Special Educational Needs and Disabilities (SEND) (PDF, 175.8 KB) –

UK Council for Child Internet Safety (UKCIS)

Sexting in schools and colleges: responding to incidents and safeguarding young people aims to support DSLs in dealing with sexting concerns

Education for a Connected World framework - describes the digital knowledge and skills that children and young people should have the opportunity to develop at different ages and stages of their lives. - Updated **30 June 2020** Added Education for a Connected World framework - 2020 edition.

Online safety in schools and colleges: Questions from the Governing Board - questions to help governing boards support their school leaders to keep children safe online – **updated June 2020**

Using External Visitors to Support Online Safety Education - helps educational settings ensure that online safety education sessions delivered by external visitors are effective.

Oakfield's E – Safety Log Incident Form –Part 1 - Appendix A

To be completed by staff member who identified the incident	
Identify person/s involved:	
Date of Incident:	
Time of Incident:	
Description of the E– safety incident: (details of incident needs to be explained in fully)	

Description of information recorded and secured	**Yes**	**No**
Have files /audio/text/images been recorded and secured? Has any computer or other technology including mobile phones been secured?		
If yes how, where, who by, and when secured?		
What actions were taken by you?		

Name of person completing this form:			
Date:		**Signature:**	

Send this completed form immediately to the Child Protection Co ordinator and Deputy Head

E -incident Log Part 1 – Member of staff identifying incident - Appendix A

Date and Time section:
Please complete all sections, if you don't know the exact day or time of the incident, please write 'unknown'

Description of the e-safety incident:
It is vital that all details you know are recorded, including how the information became known to you and from whom. If there is insufficient space on the form, please use additional sheets, but ensure that they are firmly attached and a note clearly identifies additional sheets used. Include detail of specific services or websites used if known (e.g., chat room, instant messenger); e-mail addresses; usernames etc. Give full details of real names and e-mail addresses etc. where known.

Some prompts to assist you could be:
How was the incident identified? Who was involved and how do you know this? Why do you have concerns?

Description of information recorded or secured
Legal guidance for those reporting E–SAFETY incidents that involve a criminal offence

POWERS
If any person has reasonable grounds to believe that an offence IS being committed, then they may detain the person (offender only) if safe to do so and secure any evidence of the offence (including property). This would include the property of a victim or offender. Once evidence is secured the Police may then seize the property under the Police & Criminal Evidence Act 1984.Offences committed via computers/laptops/mobile phones.
In these situations, the securing of information must be carried out in a specific way in order to obtain the best evidence possible for the police and other law enforcement agencies. When a computer is turned on or on standby it should be left exactly as it is; in order to allow a trained seizure officer to attend. In all cases; attempts should be made to record in note form any details that can be seen on the screen. DO NOT follow any links or change any pages.

Information that should be noted if on screen:

- Website address.
- Email addresses of sender and recipient.
- Dates and Times.
- User names.
- Mobile phone numbers.
- Any profile information
- Any text from chat conversations.

If inappropriate behaviour is conducted via any device or website like MSN, FACEBOOK, any 'chat' forum or social networking site. DO NOT DELETE or interfere with the offending account, (this will be done when the evidence is secured).
This will enable the police to conduct their enquiries expediently and facilitate the speedier return of seized computer equipment to their owners.

The above information is not an exhaustive list and any other information noted on screen should be included.

Actions taken
Please give full details of other agencies that have been informed. If the police have not been informed, this must be noted, together with reasons, as e-safety incidents extend well beyond 'grooming' and may be linked to other criminal activity.
This may include racist incidents, extremist radicalisation or bullying online,
The form must then be signed and dated and handed to the child protection Coordinator – Jayne Oakley and also inform Leanne Smith – Deputy Head.

Oakfield's E – Safety Log Incident Form –Part 2 – Appendix B

To be completed by Child Protection Coordinator		
Notification:		
Was notification to the Local Authority Designated Officer required?		
If Yes, what was the outcome?		
Have the Police been informed?		
Please give details (if no still give details)		
Outcome of the incident?		
Have specific vulnerabilities been identified?	**Yes**	**No**
If yes, what action will now be taken?		

Name of person completing this form:			
Date:		**Signature:**	

E-incident Log Part 2 –Responsibility for Child Protection Coordinator - Appendix B

Notifications

Please give full details of other agencies that have been informed. The person initially identifying the incident may have already contacted others, please also record them here, plus any additional action taken by you after receiving the completed Incident Log

As with Incident Log Part 1, if the police have not been informed, this must be noted, together with reasons, as e-safety incidents extend well beyond 'grooming' and may be linked to other criminal activity. This may include racist incidents, radicalisation or bullying online.

It is possible that information has not been recorded and secured by the member of staff completing Log Incident Form.

You are reminded that you have powers to detain and secure if you have reasonable grounds to believe that an offence is being committed. You may detain the person (offender only) if safe to do so and secure any evidence of the offence (including property). This would include the property of a victim or offender.

Once evidence is secured the Police may then seize the property under the Police & Criminal Evidence Act 1984. Offences committed via computers/laptops/tablets/mobile phones.

In these situations, the securing of information must be carried out in a specific way in order to obtain the best evidence possible for the police and other law enforcement agencies.

When a computer is turned on or on standby it should be left exactly as it is; in order to allow a trained seizure officer to attend. In all cases; attempts should be made to record in note form any details that can be seen on the screen. DO NOT follow any links or change any pages.

Information that should be noted if on screen

- Website address.
- Email addresses of sender and recipient.
- Dates and Times.
- User names.
- Mobile phone numbers.
- Any profile information
- Any text from chat conversations.

If inappropriate behaviour is conducted via any device or website like on MSN, FACEBOOK, any 'chat' forum or Social networking site. DO NOT DELETE or interfere with the offending account, (this will be done when the evidence is secured).

This will enable the police to conduct their enquiries expediently and facilitate the speedier return of seized computer equipment to their owners.

The above information is not an exhaustive list and any other information noted on screen should be included.

Conclusion to the incident
Please record any disciplinary action taken or communications with parents/carers or other agencies, as well as specific detail of future meetings, monitoring or discussion planned.

Vulnerabilities and Trends
If there are additional vulnerabilities and trends that have been revealed by the incident, there may be a need to review the school's policy or pass information to other agencies at a later date, either once the investigation has been concluded or even before that.
Please record all details that you are able to provide at this stage.
Please complete and sign Log Part 2 and retain in a secure location for monitoring purposes.

Appendices

Appendix A – Incident Log Part 1 and Descriptors
Appendix B – Incident Log Part 2 and Descriptors
Appendix C – Staff Acceptable Use Policy
Appendix D – Pupil Acceptable Use Policy
Appendix E – AU letter to parents
Appendix F – Flowchart

Staff Acceptable Use Policy

Data protection

- I understand that I must not disclose any password or login name to anyone, other than the persons responsible for running and maintaining the system.
- I understand that I must not allow any student to use my personal login to any of the ICT systems for ANY reason.
- I understand that pupils must not be allowed to use STAFF PCs
- I understand that I must take every reasonable precaution to secure any data or equipment removed from the school premises.
- I understand that equipment taken off site will be my personal responsibility and I am advised to check that its loss or damage is covered by my personal insurance.
- I understand that the School can and will monitor any data on the network, even if the device is NOT on school site, to ensure policy compliance, and to aid in resolving networking issues.

Use at Home

· All school equipment can be monitored through Securus even if the equipment is not on the school site.

· The school expects staff to use equipment in an appropriate manner and for appropriate uses even when outside the school site.

· Employees will maintain conduct of the highest standard such that public confidence in their integrity is sustained. – Terms and Conditions of Employment, Para 2 (2.1)

Student protection

- I am aware of all guidelines to conceal student identities when publishing to the public domain.
- I understand that students must be supervised at all times when in an ICT suite or on computer equipment.
- When arranging use of ICT facilities, I will ensure that a staff member is able to monitor pupils at all times.
- I have read and understand my role regarding acceptable use and my role in enforcing it.
- I will escalate non-compliance by students in accordance with school policy.

Reporting incidents

- I will inform a member of the network management staff in writing/verbally immediately of any websites accessible from within school I feel are unsuitable in any way for student consumption.

- I understand my part in maintaining the accuracy of the filtering system.

- I will inform a member of the network management staff in writing/verbally immediately of abuse of any ICT system(s) - software and hardware - providing the location and names where possible.
- I will inform a member of the network management staff in writing immediately of any inappropriate content suspected to be on the ICT system(s). This may be contained in email, documents, pictures etc.
- I will report any breaches, or attempted breaches, in security to a member of the network management staff in verbal/writing immediately.

Software, hardware, copyright and licensing

- I will not attempt to install any software or hardware.
- Before purchasing any hardware or software I will consult a member of the network management staff to check compatibility, license compliance and discuss any other implications that the purchase may have.
- I will respect copyright and make sure I do not use any information breaching copyright law.
- Under no circumstances must any software from potentially illegal sources be installed.

Internet and Social websites

The school recognises the massive educational potential of Web 2.0 Technologies including and not limited to Social Networking, Blogging, Micro Blogging and media sharing sites.

The school encourages staff to use these technologies but for research purposes and the sharing of good practice. In using such technologies and platforms staff should adhere to the following guide:

- Staff should not mention the school in a negative manner. This includes all stake holders' pupils, colleagues, and parents.
- Staff should refrain from commenting on incidents that occur within the school directly.

It is expected that, in all every areas of communication, staff will maintain proper professional distance from pupils currently at school: this must include rejecting requests by them to be added as friends, on all forms of social websites and taking all the measures available within the platforms to deny them access to profiles, personal information and online communications, keeping this strictly to whoever is on your allowed friends lists.

It is strongly advised you do not have past pupils on your friend's / contact lists (please seek advice from a member of the Senior Leadership Team should you need further advice)

All forms of social website access within school are currently denied.

I agree to abide by the above statements

Appendix D Acceptable Use Policy for Pupils

I understand that every time I logon to the school network I am agreeing to the Acceptable Use Policy for Pupils as described below.

<u>Using school equipment</u>

· I will respect and look after any school ICT equipment, for example laptops, cameras, keyboards etc. If I use any ICT equipment that is already damaged I will report it to my teacher.

· I will not download or install software on school equipment.

Security and safety

· I will only logon to the school network and internet with my own username and password.

· I will not reveal my passwords to anyone. I am advised to change them regularly.

· I understand that every time I logon to the internet through the school network I am agreeing to their terms and conditions.

· I will not attempt to bypass the school's internet filtering system.

· I will not give out any personal information such as my name, phone number or address on the internet.

Communication

· I will only use my school e-mail address to contact teachers.

· I will make sure that all e-mail communications with students, teachers or others is responsible and sensible.

School purposes

· I will only use the school's ICT for school purposes. This includes the internet and e-mail.

· I will only take images and audio recordings of staff/students with appropriate permission and use them for school purposes. (I understand that parents/carers are required to give their permission for images of their children to be taken and used by the school. I will respect their decision.)

Behaviour

· I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.

· I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.

· I will ensure that my online activity in and out of school will not offend or embarrass my school, the staff or students.

· I will respect the privacy and ownership of others' work on the school network and on-line at all times.

Monitoring

I know that all my computer and internet use on school equipment is monitored. I know that the monitoring software will record any images, text or keystrokes it considers inappropriate. I know that this information is available to the Leadership Team.

Accessing my school desktop from home

· I understand that the above statements still apply if I use the 'cc4anywhere' software from home to access my school desktop.

I understand that the Acceptable Use Policy is designed to help keep every member of the school community safe.

I understand that if I do not follow these rules, school sanctions will be applied and my parents/carers may be contacted.

Appendix E

Date ……

Dear Parent / Carer

Whist your child is in attendance at Oakfield School they will use computers and media devices. In order to adhere to the schools E-Safety Policy students and staff must adhere to the Acceptable Use Policy.

Attached you will find a copy of the Acceptable Use Policy. Please take the time to read this with your child and sign the detachable slip at the bottom of this letter which will need returning to the school office.

If you have any questions regarding this letter and / or questions with reference to the policy you have been provided with, please contact the school.

The attached Acceptable Use Policy if for you to keep for your reference.

Yours sincerely

Rachel Davies
Headteacher

- -

I have received and read the Acceptable Use Policy for students. I agree with its content and provide two signatures to authorise use of computers and agree to the terms

Parent / Carer name _______________________ Signature _____________________

Student Name _______________________ Signature _____________________