Online Safety Policy

Online Safety Policy

1 Our Vision for Online 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 Online 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.

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

1.6 Oakfield School's Online 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. Our responsibility is to set high expectations of our students using communication technologies and to maintain a consistent approach to Online 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 Online safety within school will be reflected within this policy.

2.3 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 Online 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 Online Safety.

3.3 Amendments to the school Online 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 Online Safety is the responsibility of the whole school community, 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 Online Safety) for all members of the school community, with day-to-day responsibility for Online Safety delegated to the Deputy Headteacher and Child Protection Coordinators.

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 Online Safety roles and to train other colleagues when necessary.

4.2.3 The Headteacher and SLT will receive timely, regular and routine updates and reports on all Online Safety incidents.

4.2.4 The team will ensure that Online Safety education is appropriately embedded across the whole curriculum.

4.2.5 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 Online Safety throughout the school.

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

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

4.3.4 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 and managed in line with this policy.

4.3.5 All staff must read, understand and actively promote the school's Online Safety policies and guidance.

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

4.4.1 Be aware of the school's Online Safety Policy and guidance.

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

4.4.3 Report any Online Safety related issues that come to their attention to the Child Protection Coordinators.

4.4.4 Develop and maintain an awareness of current Online Safety issues, legislation and guidance relevant to their work.

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

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

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

4.4.8 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.

4.5 **Pupils are required to:**

4.5.1 Understand and adhere to the Acceptable Use Policy.

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

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

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

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

4.5.6 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.

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

4.5.8 Access Online Safety lessons where students can understand and contribute to the effectiveness of the Online Safety processes.

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

4.6 **Parents/Carers are required to:**

4.6.1 Help and support the school in promoting Online Safety.

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

4.6.3 Discuss Online 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.

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

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

4.6.6 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 carers. 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.

6 Teaching & Learning

6.1 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 Online Safety risk as highlighted by Ofsted are:

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

6.1.2 **Contact** – Children 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.

6.1.3 **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.

7 In order to minimize the risks to our pupils the school will:

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

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

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

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

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

7.6 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.

7.7 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).

7.8 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.

8 Staff Training & Awareness

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

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

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

8.4 All staff will be required to incorporate Online Safety activities and awareness within their curriculum areas.

8.5 Safeguarding Level 1.

8.6 GDPR Training.

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

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

9.2 Servers and other key hardware or infrastructure will be located securely.

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

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

9.5 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.

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

10 Passwords

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

10.2 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.

10.3 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.

11 Mobiles Phone, Smart Phones & Smart Watches

11.1 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 media accounts whilst at school

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

11.3 If pupils fail to use their mobile device appropriately then a member of staff will remove their device and parents/carers will be informed.

12 Staff Use of Mobiles Devices

12.1 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.

12.2 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.

12.3 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.

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

13 Filtering Internet Access

13.1 The school filters and monitors its internet provision appropriate to the age and maturity of pupils – filtering is both externally managed (Cloud based) and internally managed with Smoothwall, by RM (ICT facilities management).

13.2

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

13.4 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.

13.5 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.

13.6 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.

13.7 The Smoothwall also sends reports to the E-Safety officers to alert them to any suspicious usage

14 Internet Access Authorisations

14.1 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 Online Safety is discussed and agreed prior to admission.

14.2 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.

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

15 Email

15.1 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.
- 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 information being revealed.
- Staff members are responsible for keeping their password secure.
- 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.
- Staff should never open attachments from an untrusted source.
- 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.

16 Use of Social Media

16.1 Staff must not talk about their professional role in any capacity when using personal social media.

16.2 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.

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

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

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

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

17 Use Memory Sticks

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

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

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

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

18 Electronic Bullying & Harassment

18.1 This Online 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: ‘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.’

19 Online Sexual Harassment

19.1 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.

19.2 Online sexual harassment 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.

19.3 Any report of online sexual harassment will be taken seriously, and the Police may be notified.

20 Sexting & School Protocols in dealing with incidents

20.1 ‘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.

20.2 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 electronically and/or adults via a mobile phone, handheld device, computer, ‘tablet’ or website with people they may not even know.

20.3 The Child Protection Coordinators and Deputy Child Protection Coordinator need to be informed of any 'sexting' incidents.

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

20.4.1 'Sexting' disclosures should follow the normal safeguarding practices and protocols (refer to the school's Child Protection Policy).

20.4.2 Staff will engage and offer support to the pupil affected.

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

20.4.4 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?
- Is it a school device or a personal device?
- Does the pupil need immediate support and/or protection?
- Are there other pupils involved?

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

Never:

- Search a mobile device, even in response to an allegation or disclosure.
- 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

Viewing inappropriate material could place yourself at risk and you could be breaking the law. Always seek advice from Safeguarding Leads.

20.5 **Step 2 – Who should deal with the incident?**

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

20.5.2 All safeguarding and Online Safety incidents should be reported to the Child Protection Coordinators and the Deputy Child Protection Coordinator who will then deal with the incident.

20.5.3 The Child Protection Coordinators will initiate safeguarding Procedures. The Headteacher and or Deputy Head should also always be informed- usually by the Child Protection Coordinators.

20.6 **Step 3 – Deciding on a response**

20.6.1 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.

20.6.2 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.

20.6.3 If indecent images of a pupil / young person are disclosed:

- Act in accordance with the Child Protection Policy/Procedures i.e. inform the Child Protection Coordinators.
- 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.
- The safeguarding team will inform parents and/or carers (where appropriate) about the incident and how it is being managed.

20.7 **Step 4 – Containment and Prevention**

20.7.1 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.

20.7.2 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.

20.7.3 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/carers 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.

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

21 Dealing with Incidents

21.1 An important element of Online Safety 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 Online Safety incidents so that they may be dealt with effectively and in a timely manner in order to minimise any impact.

21.2 When incidents have been reported, the Child Protection Coordinators/ Deputy Child Protection Coordinator and the Deputy Head will decide what action will be taken.

21.3 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.

22 Evaluating the Impact of this Online Safety Policy

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

22.2 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 Online Safety Policy is adequate and that the implementation of the Online 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.

23 Radicalisation Procedures & Monitoring

23.1 We will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school and that suitable filtering is in place which considers the needs of pupils.

23.2 When concerns are noted by staff that a pupil may be at risk of radicalisation online then the Child Protection Coordinators will be informed immediately, and action will be taken in line with the School's Child Protection/Safeguarding Policy.

24 Monitoring & Review

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

24.2 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 2022

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

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.

Appendices

Appendix A – Staff Acceptable Use Policy
Appendix B – Pupil Acceptable Use Policy

Appendix A

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 B

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.

Using school equipment

· 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.