

## ONLINE SAFETY AND ACCEPTABLE USE OF TECHNOLOGY POLICY & PROCEDURE

<b>Date of last review</b>	September 2020
<b>Date of next review</b>	September 2021

# Contents

	<b>Page no</b>
1. Policy Aims	2
2. Policy Scope	2
2.2 Links with other policies and practices	2
3. Monitoring and Review	3
4. Roles and Responsibilities	3
4.1 The leadership and management team	3
4.2 The Designated Safeguarding Lead	3
4.3 members of staff	4
4.4 Staff who manage the technical environment	4
4.5 Pupils	4
4.6 Parents	5
5. Education and Engagement Approaches	5
5.1 Education and engagement with pupils (including vulnerable pupils)	5
5.2 Training and engagement with staff	6
5.3 Awareness and engagement with parents	6
6. Reducing Online Risks	6
7. Safer Use of Technology	7
7.1 Classroom Use	7
7.2 Managing Internet Access	7
7.3 Filtering and Monitoring	7
7.4 Managing Personal Data Online	8
7.5 Security and Management of Information Systems	8
7.6 Managing the Safety of the School Website	9
7.7 Publishing Images and Videos Online	10
7.8 Managing Email	10
7.9 Management of Applications (apps) used to Record Children's Progress	10
8. Social Media	11
8.1 Expectations	11
8.2 Staff Personal Use of Social Media	11
8.3 Pupils' Personal Use of Social Media	12
8.4 Official Use of Social Media	13
9. Use of Personal Devices and Mobile Phones	14
9.1 Expectations	14
9.2 Staff Use of Personal Devices and Mobile Phones	15
9.3 Pupils' Use of Personal Devices and Mobile Phones	16
9.4 Visitors' Use of Personal Devices and Mobile Phones	16
9.5 Officially provided mobile phones and devices	16
10. Responding to Online Safety Incidents and Concerns	17
10.1 Concerns about Pupils Welfare	17
10.2 Staff Misuse	17
11. Procedures for Responding to Specific Online Incidents or Concerns	17
11.1 Youth Produced Sexual Imagery or "Sexting"	17
11.2 Online Child Sexual Abuse and Exploitation	19
11.3 Indecent Images of Children (IIOC)	20
11.4 Cyberbullying	20
11.5 Online Hate	20
11.6 Online Radicalisation and Extremism	20
12. Useful Links for Educational Settings	21

## ONLINE SAFETY AND ACCEPTABLE USE OF TECHNOLOGY POLICY & PROCEDURE

---

### 1. Policy Aims

- This online safety policy has been written by Oyster Park Primary Academy, it takes into account the DfE statutory guidance Keeping Children Safe in Education 2020 and Early Years and Foundation Stage 2017
- The purpose of Oyster Park Primary Academy's online safety policy is to:
  - Safeguard and protect all members of our school community online.
  - Identify approaches to educate and raise awareness of online safety throughout the community.
  - Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
  - Identify clear procedures to use when responding to online safety concerns.
- Oyster Park Primary Academy identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:
  - **Content:** being exposed to illegal, inappropriate or harmful material
  - **Contact:** being subjected to harmful online interaction with other users
  - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

### 2. Policy Scope

- Oyster Park Primary Academy believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm online.
- We identify that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- Oyster Park Primary Academy believes that pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as pupils and parents/carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with school issued devices for use off-site, such as work laptops, tablets or mobile phones.

#### 2.2 Links with other policies and practices

- This policy links with a number of other policies, practices and action plans including:
  - Anti-bullying policy
  - Acceptable Use Policies (AUP) and/or the Code of conduct
  - Behaviour policy
  - Safeguarding and Child protection policy
  - Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE) and Sex and Relationships Education (SRE)
  - Image use policy

### 3. Monitoring and Review

- Oyster Park Primary Academy will review this policy at least annually

## ONLINE SAFETY AND ACCEPTABLE USE OF TECHNOLOGY POLICY & PROCEDURE

---

- The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure
- We will ensure that we regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the headteacher will be informed of online safety concerns, as appropriate.
- The named Governor for safeguarding will report on a regular basis to the governing body on online safety incidents, including outcomes.
- Any issues identified will be incorporated into the school's action planning.

### **4. Roles and Responsibilities**

- The school has appointed Hilary Bodycombe, as Designated Safeguarding Lead to be the online safety lead.
- Oyster Park Primary Academy recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

#### **4.1 The leadership and management team will:**

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a Code of conduct and/or an AUP, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place.
- Work with technical staff to monitor the safety and security of school systems and networks.
- Ensure that online safety is embedded within a progressive whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.
- Support the Designated Safeguarding Lead by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology. Audit and evaluate online safety practice to identify strengths and areas for improvement.

#### **4.2 The Designated Safeguarding Lead (DSL) will:**

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the schools safeguarding recording mechanisms.

## ONLINE SAFETY AND ACCEPTABLE USE OF TECHNOLOGY POLICY & PROCEDURE

---

- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the management team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly with the governor with a lead responsibility for safeguarding and online safety.

### **4.3 It is the responsibility of all members of staff to:**

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and AUPs.
- Take responsibility for the security of school systems and the data they use, or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

### **4.4 It is the responsibility of staff managing the technical environment to:**

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures (*including password policies and encryption*) to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that the schools filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Report any filtering breaches to the DSL and leadership team, as well as, the school's Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the school's safeguarding procedures.

### **4.5 It is the responsibility of pupils (at a level that is appropriate to their individual age, ability and vulnerabilities) to:**

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the school's Acceptable Use Policy.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.

## ONLINE SAFETY AND ACCEPTABLE USE OF TECHNOLOGY POLICY & PROCEDURE

---

- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

### **4.6 It is the responsibility of parents and carers to:**

- Read the school AUPs and encourage their children to adhere to them.
- Support the school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the school's AUPs. Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the school online safety policies.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

## **5. Education and Engagement Approaches**

### **5.1 Education and engagement with pupils**

- The school will establish and embed a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst pupils by:
  - Ensuring education regarding safe and responsible use precedes internet access.
  - Including online safety in the PSHE/Social Skills, SRE and Computing programmes of study, covering use both at school and home.
  - Reinforcing online safety messages whenever technology or the internet is in use.
  - Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
  - Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The school will support pupils to read and understand the AUP in a way which suits their age and ability by:
  - Displaying acceptable use posters in all rooms with internet access.
  - Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
  - Rewarding positive use of technology by pupils.
  - Seeking pupil voice when writing and developing school online safety policies and practices, including curriculum development and implementation.
  - Using support, such as external visitors, where appropriate, to complement and support the schools internal online safety education approaches.

#### **5.1.1 Vulnerable Pupils**

- Oyster Park Primary Academy is aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special

## ONLINE SAFETY AND ACCEPTABLE USE OF TECHNOLOGY POLICY & PROCEDURE

---

Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

- Oyster Park Primary Academy will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils
- Oyster Park Primary Academy will seek input from specialist staff as appropriate, including the SENCO and LAC Lead.

### **5.2 Training and engagement with staff**

The school will:

- Provide and discuss the online safety policy with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates.
  - This will cover the potential risks posed to pupils (Content, Contact and Conduct) as well as our professional practice expectations.
- Make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

### **5.3 Awareness and engagement with parents and careers**

- Oyster Park Primary Academy recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.
- The school will build a partnership approach to online safety with parents and carers by:
  - Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness information and highlighting online safety at other events such as parent evenings, curriculum evenings and transition events.
  - Drawing their attention to the school online safety policy and expectations in newsletters, letters, our prospectus and on our website.
  - Requesting that they read online safety information as part of joining our school, for example, within our induction packs.
  - Requiring them to read the school AUP and discuss its implications with their children.

## **6. Reducing Online Risks**

- Oyster Park Primary Academy recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:
  - Regularly review the methods used to identify, assess and minimise online risks.
  - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted.

## ONLINE SAFETY AND ACCEPTABLE USE OF TECHNOLOGY POLICY & PROCEDURE

---

- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a school computer or device.
- All members of the school community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the school's AUP and highlighted through a variety of education and training approaches.

### **7. Safer Use of Technology**

#### **7.1 Classroom Use**

- Oyster Park Primary Academy uses a wide range of technology. This includes access to:
  - Computers, laptops and other digital devices
  - Internet which may include search engines and educational websites
  - Email
  - Games consoles and other games based technologies
  - Digital cameras, web cams and video cameras
- All school owned devices will be used in accordance with the school's AUP and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The school will ensure that the use of internet-derived materials, by staff and pupils, complies with copyright law and acknowledge the source of information.
- Supervision of pupils will be appropriate to their age and ability.
  - **Early Years Foundation Stage and Key Stage 1**
    - Pupils' access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the pupils' age and ability.
  - **Key Stage 2**
    - Pupils will use age-appropriate search engines and online tools.
    - Children will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' age and ability.

#### **7.2 Managing Internet Access**

- The school will maintain a written record of users who are granted access to the school's devices and systems.
- All staff, pupils and visitors will read and sign an AUP before being given access to the school computer system, IT resources or internet.

#### **7.3 Filtering and Monitoring**

- The school's filtering and monitoring systems and processes will be managed by MINT who are employed to manage the school's technical environment

## ONLINE SAFETY AND ACCEPTABLE USE OF TECHNOLOGY POLICY & PROCEDURE

---

**Note: A guide for education settings about establishing 'appropriate levels' of filtering and monitoring can be found at: [www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring](http://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring)**

### **7.3.1 Decision Making**

- Oyster Park Primary Academy governors and leaders have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

### **7.3.2 Filtering**

- The school uses educational broadband connectivity through Alamo
  - The school uses Alamo Safety which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
  - The school filtering system blocks all sites on the [Internet Watch Foundation](#) (IWF) list.
- The school works with MINT to ensure that our filtering policy is continually reviewed.

#### *Dealing with Filtering breaches*

- The school has a clear procedure for reporting filtering breaches.
  - If pupils discover unsuitable sites, they will be required to turn off the monitor/screen and report the concern immediate to a member of staff.
  - The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead and/or technical staff.
  - The breach will be recorded and escalated as appropriate.
  - Parents/carers will be informed of filtering breaches involving their child.
- Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as: Wakefield Police or CEOP.

### **7.3.4 Monitoring**

- The school will appropriately monitor internet use on all school owned or provided internet enabled devices. This is achieved by:
  - physical monitoring (supervision),
  - monitoring internet and web access (reviewing log file information)
- The school will respond immediately to concerns identified via monitoring approaches
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

## ONLINE SAFETY AND ACCEPTABLE USE OF TECHNOLOGY POLICY & PROCEDURE

---

### **7.4 Managing Personal Data Online**

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations (GDPR) and Data Protection legislation.
  - Full information can be found in the GDPR policy

### **7.5 Security and Management of Information Systems**

- The school takes appropriate steps to ensure the security of our information systems, including:
  - Virus protection being updated regularly.
  - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
  - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
  - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
  - Regularly checking files held on the school's network,
  - The appropriate use of user logins and passwords to access the school network.
    - Specific user logins and passwords will be enforced for all
  - All users are expected to log off or lock their screens/devices if systems are unattended.

#### **7.5.1 Password policy**

- All members of staff will have their own unique username and private passwords to access school systems; members of staff are responsible for keeping their password private.
- All pupils are provided with their own unique username and private passwords to access school systems; pupils are responsible for keeping their password private.
- We require staff to:
  - Use strong passwords for access into our system.
  - Change their passwords regularly
  - Always keep their password private; users must not share it with others or leave it where others can find it.
  - Not to login as another user at any time.

### **7.6 Managing the Safety of the School Website**

- The school will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- The school will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or pupils' personal information will not be published on our website; the contact details on the website will be the school address, email and telephone number.
- The administrator account for the school website will be secured with an appropriately strong password.

## ONLINE SAFETY AND ACCEPTABLE USE OF TECHNOLOGY POLICY & PROCEDURE

---

- The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community.

### **7.7 Publishing Images and Videos Online**

- The school will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to): the Image use policy, Data security, AUPs and Codes of conduct.

### **7.8 Managing Email**

- Access to school email systems will always take place in accordance with Data protection legislation and in line with other school policies, including: Confidentiality, AUPs and Code of conduct.
  - The forwarding of any chain messages/emails is not permitted. Spam or junk mail will be blocked and reported to the email provider.
  - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
  - School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the school community will immediately tell the DSL if they receive offensive communication, and this will be recorded in the school safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked in school.

#### **7.8.1 Staff**

- The use of personal email addresses by staff for any official school business is not permitted.
  - All members of staff are provided with a specific school email address, to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email.

#### **7.8.2 Pupils**

- Pupils will use school provided email accounts for educational purposes.
- Pupils will sign an AUP and will receive education regarding safe and appropriate email etiquette before access is permitted.

### **7.9 Management of Applications which Record Children's Progress**

- The school uses Target Tracker to track pupils progress and share appropriate information with parents and carers.
- The headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that tracking systems are appropriately risk assessed prior to use, and that they are used in accordance with GDPR and data protection legislation
- To safeguard data:
  - Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs. Personal staff mobile phones or devices will not be used to access or upload content.

## ONLINE SAFETY AND ACCEPTABLE USE OF TECHNOLOGY POLICY & PROCEDURE

---

- School devices will be appropriately encrypted if taken off site to reduce the risk of a data security breach in the event of loss or theft.
- All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
- Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

### **8. Social Media**

#### **8.1 Expectations**

- The expectations' regarding safe and responsible use of social media applies to all members of Oyster Park Primary Academy community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of Oyster Park Primary Academy community are expected to engage in social media in a positive, safe and responsible manner, at all times.
  - All members of Oyster Park Primary Academy community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The school will control pupil and staff access to social media whilst using school provided devices and systems on site
  - The use of social media during school hours for personal use **is not** permitted.
  - Inappropriate or excessive use of social media during school/work hours or whilst using school devices may result in disciplinary or legal action and removal of internet facilities.
- Concerns regarding the online conduct of any member of Oyster Park Primary Academy community on social media, should be reported to the school and will be managed in accordance with our Anti-bullying, Allegations against staff, Behaviour and Child protection policies.

#### **8.2 Staff Personal Use of Social Media**

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Code of conduct within the AUP.

#### ***Reputation***

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within school. Civil, legal or disciplinary action may be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
  - Setting the privacy levels of their personal sites as strictly as they can.
  - Being aware of location sharing services.
  - Opting out of public listings on social networking sites.

## ONLINE SAFETY AND ACCEPTABLE USE OF TECHNOLOGY POLICY & PROCEDURE

---

- Logging out of accounts after use.
- Keeping passwords safe and confidential.
- Ensuring staff do not represent their personal views as that of the school.
- Members of staff are encouraged not to identify themselves as employees of Oyster Park Primary Academy on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with schools policies and the wider professional and legal framework.
  - Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role in the school.

### ***Communicating with pupils and parents and carers***

- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles.
  - Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the headteacher.
  - If ongoing contact with pupils is required once they have left the school roll, members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.
- Any communication from pupils and parents received on personal social media accounts will be reported to the schools Designated Safeguarding Lead.

### **8.3 Pupils' Personal Use of Social Media**

- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts specifically for children under this age.
- Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.
- Pupils will be advised:
  - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples could include real/full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.

## ONLINE SAFETY AND ACCEPTABLE USE OF TECHNOLOGY POLICY & PROCEDURE

---

- To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- To use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications and report concerns both within school and externally.

### **8.4 Official Use of Social Media**

- *Oyster Park Primary Academy* official social media channels are:
  - **Twitter**
  - **Facebook**
- The official use of social media sites, by the school, only takes place with clear educational or community engagement objectives, with specific intended outcomes.
  - The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher.
  - Leadership staff have access to account information and login details for the social media channels, in case of emergency, such as staff absence.
- Official school social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
  - Staff use school provided email addresses to register for and manage any official school social media channels.
  - Official social media sites are suitably protected
  - Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including: Anti-bullying, Image use, Data protection, Confidentiality and Child protection.
  - All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents, carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
  - Social media tools Twitter and Facebook which have been risk assessed and approved as suitable for educational purposes will be used.
  - Any official social media activity involving pupils will be moderated by the school where possible.
- Parents and carers will be informed of any official social media use with pupils and written parental consent will be obtained, as required.
- The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

### ***Staff expectations***

- Members of staff who follow and/or like the school social media channels will be advised to do so professionally and not engage in any communication with parents

## **ONLINE SAFETY AND ACCEPTABLE USE OF TECHNOLOGY POLICY & PROCEDURE**

---

- If members of staff are participating in online social media activity as part of their capacity as an employee of the school, they will:
  - Sign the school's Social media acceptable use policy.
  - Be professional at all times and aware that they are an ambassador for the school.
  - Disclose their official role and/or position, but make it clear that they do not necessarily speak on behalf of the school.
  - Be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
  - Always act within the legal frameworks they would adhere to within the workplace, including: Libel, Defamation, Confidentiality, Copyright, Data protection and Equalities laws.
  - Ensure that they have appropriate written consent before posting images on the official social media channel.
  - Not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
  - Not engage with any direct or private messaging with current, or past, pupils, parents and carers.
  - Inform their line manager, the Designated Safeguarding Lead and/or the Headteacher of any concerns, such as criticism, inappropriate content or contact from pupils.

### **9. Use of Personal Devices and Mobile Phones**

- Oyster Park Primary Academy recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within school.

#### **9.1 Expectations**

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies, including, but not limited to: Anti-bullying, Behaviour and Safeguarding and Child protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user at all times.
  - All members of Oyster Park Primary Academy community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; the school accepts no responsibility for the loss, theft or damage of such items on school premises.
  - All members of the school community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used in specific areas within the school site such as changing room and toilets
- The sending of abusive or inappropriate messages/ content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our Behaviour policy.
- All members of Oyster Park Primary Academy community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school Behaviour or Safeguarding and Child protection policies.

## ONLINE SAFETY AND ACCEPTABLE USE OF TECHNOLOGY POLICY & PROCEDURE

---

### **9.2 Staff Use of Personal Devices and Mobile Phones**

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant school policy and procedures, such as: Confidentiality, Safeguarding and Child protection, Data security and Acceptable use.
- Staff will be advised to:
  - Keep mobile phones and personal devices in a safe and secure place during lesson time
  - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
  - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
  - Not use personal devices during teaching periods, unless permission has been given by the Headteacher, such as in emergency circumstances.
  - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers.
  - Any pre-existing relationships, which could undermine this, will be discussed with the Designated Safeguarding Lead and Headteacher.
- Staff will not use personal devices, such as: mobile phones, tablets or cameras:
  - To take photos or videos of pupils and will only use work-provided equipment for this purpose.
  - To communicate directly with pupils, and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches the school policy, action will be taken in line with the school behaviour and allegations policy
  - If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

### **9.3 Pupils' Use of Personal Devices and Mobile Phones**

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- Oyster Park Primary Academy expects pupil's personal devices and mobile phones to be handed into the school office on arrival to school and collected at the end of the school day. (See Mobile Phone Policy)
- If a pupil needs to contact his/her parents or carers they will be allowed to use a school phone.
  - Parents are advised to contact their child via the school office during school hours.
- Mobile phones or personal devices will not be used by pupils during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff.
  - The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
  - If members of staff have an educational reason to allow children to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the Leadership Team.
- Mobile phones and personal devices must not be taken into examinations.

## ONLINE SAFETY AND ACCEPTABLE USE OF TECHNOLOGY POLICY & PROCEDURE

---

- Pupils found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- If a pupil breaches the school policy, the phone or device will be confiscated and will be held in a secure place.
  - School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the school's Behaviour or Bullying policy, or could contain youth produced sexual imagery (sexting).
  - Pupils' mobile phones or devices may be searched by a member of the leadership team, with the consent of the pupil or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes school policies.
  - Mobile phones and devices that have been confiscated will be released to parents or carers at the end of the school day.
  - If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

### **9.4 Visitors' Use of Personal Devices and Mobile Phones**

- Parents, carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the school's Acceptable use policy and other associated policies, such as: Anti-bullying, Behaviour, Safeguarding and Child protection and Image use.
- The school will ensure appropriate signage and information is provided to inform parents, carers and visitors of expectations of use. – do we add in visitors leaflet we need?
- Members of staff are expected to challenge visitors if they have concerns and will always inform the Designated Safeguarding Lead of any breaches of school policy.

### **9.5 Officially provided mobile phones and devices**

- Members of staff will be issued with a work phone number when appropriate for example school trips
- School mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
- School mobile phones and devices will always be used in accordance with the Acceptable use policy, Images Policy and Safeguarding and Child Protection Policy.

## **10. Responding to Online Safety Incidents and Concerns**

- All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns.
  - Pupils, parents and staff will be informed of the school's complaints procedure and staff will be made aware of the whistleblowing procedure.
- The school requires staff, parents, carers and pupils to work in partnership to resolve online safety issues.

## ONLINE SAFETY AND ACCEPTABLE USE OF TECHNOLOGY POLICY & PROCEDURE

---

- After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the Education Safeguarding Team.
- Where there is suspicion that illegal activity has taken place, the school will contact the Education Safeguarding Team or Wakefield Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with Wakefield Police and/or the Education Safeguarding Team first, to ensure that potential investigations are not compromised.

### **10.1 Concerns about Pupils Welfare**

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns.
  - The DSL will record these issues in line with the school's Safeguarding and Child Protection policy.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies
- The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

### **10.2 Staff Misuse**

- Any complaint about staff misuse will be referred to the Headteacher, according to the Allegations policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with the Behaviour policy and Code of conduct.

## **11. Procedures for Responding to Specific Online Incidents or Concerns**

### **11.1 Youth Produced Sexual Imagery or "Sexting"**

- Oyster Park Primary Academy recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; therefore all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The school will follow the advice as set out in the non-statutory UKCCIS guidance: ['Sexting in schools and colleges: responding to incidents and safeguarding young people'](#)
- Oyster Park Primary Academy will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

## ONLINE SAFETY AND ACCEPTABLE USE OF TECHNOLOGY POLICY & PROCEDURE

---

### 11.1.1 Dealing with 'Sexting'

- If the school are made aware of an incident involving the creation or distribution of youth produced sexual imagery, the school will:
  - Act in accordance with our Safeguarding and Child protection and Safeguarding policies.
  - Immediately notify the Designated Safeguarding Lead.
  - Store the device securely.
    - If an indecent image has been taken or shared on the school network or devices, the school will take action to block access to all users and isolate the image.
  - Carry out a risk assessment which considers any vulnerability of pupil(s) involved; including carrying out relevant checks with other agencies.
  - Inform parents and carers, if appropriate, about the incident and how it is being managed.
  - Make a referral to Children's Services and/or the Police, as appropriate.
  - Provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
  - Implement appropriate sanctions in accordance with the school's Behaviour policy, but taking care not to further traumatise victims where possible.
  - Consider the deletion of images in accordance with the UKCCIS: ['Sexting in schools and colleges: responding to incidents and safeguarding young people'](#) guidance.
    - Images will only be deleted once the school has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
  - Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.
- The school will take action regarding youth produced sexual imagery, regardless of whether the incident took place on/off school premises, using school or personal equipment.
- The school will not:
  - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
    - In this case, the image will only be viewed by the Designated Safeguarding Lead and their justification for viewing the image will be clearly documented.
  - Send, share, save or make copies of content suspected to be an indecent image of children (i.e. youth produced sexual imagery) and will not allow or request pupils to do so.

### 11.2 Online Child Sexual Abuse and Exploitation

- Oyster Park Primary Academy will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- We recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for pupils, staff and parents/carers.
- The school will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally.

## ONLINE SAFETY AND ACCEPTABLE USE OF TECHNOLOGY POLICY & PROCEDURE

---

### **11.2. 1 Dealing with Online Child Sexual Abuse and Exploitation**

- If the school are made aware of incident involving online sexual abuse of a child, the school will:
  - Act in accordance with the school's Child protection and Safeguarding policies
  - Immediately notify the Designated Safeguarding Lead.
  - Store any devices involved securely.
  - Immediately inform Wakefield police via 101 (or 999 if a child is at immediate risk)
  - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
  - Inform parents/carers about the incident and how it is being managed.
  - Make a referral to Children's Services (if required/ appropriate).
  - Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
  - Review the handling of any incidents to ensure that best practice is implemented; school leadership team will review and update any management procedures, where necessary.
- The school will take action regarding online child sexual abuse, regardless of whether the incident took place on/off school premises, using school or personal equipment.
  - Where possible pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report : [www.ceop.police.uk/safety-centre/](http://www.ceop.police.uk/safety-centre/)
- If the school is unclear whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Wakefiled Police.
- If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the [Child Sexual Exploitation Team](#) (CSET) by the Designated Safeguarding Lead.
- If pupils at other schools are believed to have been targeted, the school will seek support from Wakefiled Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

### **11.3 Indecent Images of Children (IIOC)**

- Oyster Park Primary Academy will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- The school will take action regarding IIOC on school equipment and/or personal equipment, even if access took place off site.
- The school will take action to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If the school is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through Wakefiled Police and/or the Education Safeguarding Team.
- If made aware of IIOC, the school will:
  - Act in accordance with the schools child protection and safeguarding policy
  - Immediately notify the school Designated Safeguard Lead.
  - Store any devices involved securely.

## ONLINE SAFETY AND ACCEPTABLE USE OF TECHNOLOGY POLICY & PROCEDURE

---

- Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Wakefield police or the LADO.
- If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet, the school will:
  - Ensure that the Designated Safeguard Lead is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via [www.iwf.org.uk](http://www.iwf.org.uk).
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Report concerns, as appropriate to parents and carers.
- If made aware that indecent images of children have been found on the school devices, the school will:
  - Ensure that the Designated Safeguard Lead is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via [www.iwf.org.uk](http://www.iwf.org.uk).
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
  - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
  - Report concerns, as appropriate to parents and carers.
- If made aware that a member of staff is in possession of indecent images of children on school devices, the school will:
  - Ensure that the Headteacher is informed.
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
  - Quarantine any devices until police advice has been sought.

### **11.4 Cyberbullying**

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Oyster Park Primary Academy.
- Full details of how the school will respond to cyberbullying are set out in the Anti-bullying policy.

### **11.5 Online Hate**

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Oyster Park Primary Academy and will be responded to in line with existing school policies, including Anti-bullying and Behaviour.
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If the school is unclear on how to respond, or whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice through the Education Safeguarding Team and/or Wakefield Police.

## ONLINE SAFETY AND ACCEPTABLE USE OF TECHNOLOGY POLICY & PROCEDURE

---

### **11.6 Online Radicalisation and Extremism**

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school.
- If the school is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately and action will be taken in line with the Safeguarding Child protection policy.
- If the school is concerned that member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately and action will be taken in line with the Safeguarding and Child protection and Allegations policies.

### **12. Useful Links for Educational Settings**

- Action Fraud: [www.actionfraud.police.uk](http://www.actionfraud.police.uk)
- CEOP:
  - [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)
  - [www.ceop.police.uk](http://www.ceop.police.uk)
- Childnet: [www.childnet.com](http://www.childnet.com)
- Get Safe Online: [www.getsafeonline.org](http://www.getsafeonline.org)
- Internet Matters: [www.internetmatters.org](http://www.internetmatters.org)
- Internet Watch Foundation (IWF): [www.iwf.org.uk](http://www.iwf.org.uk)
- Lucy Faithfull Foundation: [www.lucyfaithfull.org](http://www.lucyfaithfull.org)
- NSPCC: [www.nspcc.org.uk/onlinesafety](http://www.nspcc.org.uk/onlinesafety)
  - ChildLine: [www.childline.org.uk](http://www.childline.org.uk)
  - Net Aware: [www.net-aware.org.uk](http://www.net-aware.org.uk)
- The Marie Collins Foundation: [www.mariecollinsfoundation.org.uk](http://www.mariecollinsfoundation.org.uk)
- UK Safer Internet Centre: [www.saferinternet.org.uk](http://www.saferinternet.org.uk)
  - Professional Online Safety Helpline: [www.saferinternet.org.uk/about/helpline](http://www.saferinternet.org.uk/about/helpline)
- 360 Safe Self-Review tool for schools: [www.360safe.org.uk](http://www.360safe.org.uk)

## ONLINE SAFETY AND ACCEPTABLE USE OF TECHNOLOGY POLICY & PROCEDURE

---

### APPENDIX 1 STAFF ACCEPTABLE USE AGREEMENT

To ensure that staff are fully aware of their professional responsibilities when using digital technology, they are asked to sign this Acceptable Use Agreement. Staff should refer to the school's full Online Safety policy and procedures for further information and clarification.

#### **When using online technology in my professional capacity or for school sanctioned personal use, I understand that:**

- I must use school systems in a responsible way, to minimise the risk to my safety and to the safety and security of the systems and other users.
- The expectations set out in this Acceptable Use Agreement and the Online Safety policy, apply not only to my work and use of school digital technology equipment in school, but also apply to my use of these technologies out of school and my use of personal equipment on the premises or in situations related to my employment by the school
- My use of the Internet, email and other related technologies can be monitored and logged by school where it believes unauthorised use of the schools information system may be taking place or the system may be being used for unauthorised or unlawful purposes.
- I am responsible for my actions in and out of the school and could be subject to disciplinary action and in the event of illegal activities, the involvement of the police, for not abiding by School's expectations

#### **Security of systems and equipment**

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school.

- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may access it.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will not attempt to install or store software, or try to alter computer settings without permission and technical advice.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not disable or damage school equipment, or the equipment belonging to others.
- I will look after equipment loaned to me and for insurance purposes I will not leave it unattended in a car. I will immediately report any damage or faults involving equipment or software, however this may have happened.
- When I use my personal mobile devices (eg laptop/tablet/phone/USB devices) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use mobile phones or the internet for personal use during working hours

#### **Appropriate Use**

- I will only use the school digital technology systems and accounts or any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.

## ONLINE SAFETY AND ACCEPTABLE USE OF TECHNOLOGY POLICY & PROCEDURE

---

- I will ensure that my online activity and use of digital technology, both in school and outside school, will always be compatible with my professional role and will not bring my professional role or the School, into disrepute.
- I will not try to browse, download, upload or distribute any material that could be considered offensive, illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act), discriminatory, inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will respect copyright and intellectual property rights. Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I will report any accidental access to inappropriate materials immediately.
- I will report any illegal, inappropriate or harmful material or incident, I become aware of, immediately
- I will report any incidents of concern regarding children's safety immediately
- I will ensure children are always supervised by a responsible adult when online
- I will ensure that when I take, store or use images of others I will do so for professional purposes and in line with the school's policy on the use of images. I will not use my personal equipment to record these images, unless I have permission to do so.
- I will ensure that in line with Data Protection, any staff or pupil data to which I have access, will be kept private and confidential, stored securely and is used appropriately whether in school taken off the school premises or accessed remotely.

### Communications

- I will ensure that any electronic communications are compatible with my professional role
- I will be professional in my communications and actions when using school systems and accounts. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will only use the school system and accounts for any communications with children, parents and for other school related communications. Any such communication will be professional in tone and manner.
- I will only use social networking sites in school in accordance with the school's policies and guidance
- I will not give out my own personal details, such as mobile phone number or personal email address, to pupils or parents.

I will support and promote the school's Online Safety policy and help children to be safe and responsible in their use of digital technologies.

I have read and understand the above and agree to use the school digital technology systems, both in and out of school, and my own devices, in school and when carrying out communications related to the school, within these guidelines.

**Staff Name:**

**Signed:**

**Date:**

**APPENDIX 2****PERSONAL USE: ADVICE FOR STAFF**

**We recognise that staff use social networking sites in their own personal time and for their own personal use. However, there are still appropriate boundaries around professional conduct and interaction with pupils and parents/carers, which staff should bear in mind.**

- Posting information or views cannot be isolated from your working life. Staff must be aware that even when acting as an individual outside of school, their actions could be criticised and seen as bringing their professional status and the school into disrepute, especially if other users are aware of their role.
- Privacy on the internet rarely means communications are entirely private, even messaging. Once content is shared online it is possible for it be circulated far wider than intended without consent or knowledge.
- No reference should be made in social media to pupils, parents/carers or school staff
- Do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the School or Trust
- Examples of inappropriate materials and actions which breach trust and confidence in professionals are:
  - Posting unprofessional comments about your role or profession
  - Making derogatory comments about pupils, colleagues, the School or Trust
  - Posting offensive, harassing threatening or bullying comments about colleagues on social networking sites
  - Making inappropriate statements or using offensive or hate based language

It is an offence in law to send indecent, offensive, harassing or threatening messages which cause the recipient distress and bringing the school or profession into disrepute is a disciplinary issue.

- When publishing information about yourself or having conversations with others online, be mindful of how you present yourself, who can see your content, and how you can manage this appropriately. When publishing information, personal contact details, video or images, ask yourself if you would feel comfortable about a current or prospective employer, colleague, pupil or parent, viewing your content.
- Staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles.

Staff may want to add current and ex-pupils as friends with good intentions, for example offering support, or keeping in touch through the next stages of their life but such actions could be putting staff in a vulnerable position through risks of:

- Giving access to and sharing their personal information such as photos or comments which can be misinterpreted and shared without their knowledge or consent.
- Having access to personal information about pupils which could lead to possible concerns for example if pupils post unsuitable content or material.
- Undermining their professional reputation, as ex-pupils may have friends or other family members who are still pupils at the school.

## ONLINE SAFETY AND ACCEPTABLE USE OF TECHNOLOGY POLICY & PROCEDURE

---

- Being open to allegations of inappropriate contact or conduct and of being exposed to unwanted contact and harassment from others.

School recognises that in some cases, there may be pre-existing or external relationships which make it difficult to have a blanket ban on this. However, staff must protect themselves from any potential allegations or misinterpretation and ensure that their contact and conduct at all times is compatible with their professional role.

It is advisable to make the Online Safety Lead and SLT aware of any such relationships and contacts.

- School has the right to monitor the use of the School computer systems, including access to websites, the interception of email and the deletion of inappropriate materials, without the consent of the staff member.

### **Advice on Twitter/Facebook Use**

Regularly check security settings on personal social media profiles to minimise the risk of loss of personal information

To ensure that you are safe and protected as professionals:

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

**ONLINE SAFETY AND ACCEPTABLE USE OF TECHNOLOGY  
POLICY & PROCEDURE**

**APPENDIX 4  
RESPONDING TO INCIDENTS OF MISUSE**

If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the flowchart and report immediately to the police

