Wellfield Middle School

Online Safety Policy
September 2018

School Online Safety Policy

Wellfield Middle School has an appointed Online Safety Coordinator (Rhian Thomas-Nash, Computing subject coordinator). The Designated Child Protection Officer is Susan Winter (Head Teacher) and the Deputy Child Protection Officers are Caroline Kemp (Deputy Head Teacher), Jenny Hawkridge (Assistant Head Teacher) and Hayley McElderry (Key Stage 2 Manager). The on-site computer technician is Bev Stephenson.

Our Online Safety Policy has been written by the computing subject leader, computer technician and Senior Leadership Team (SLT) and seeks to incorporate the current government guidance. It has been agreed by the SLT and is pending approval by the school governing body in November 2017.

The Online Safety Policy for Wellfield Middle School will be reviewed annually. This policy will next be reviewed in November 2018.

Why is Internet Use Important at Wellfield?

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and is a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality internet access.

We are aware that pupils actively use the internet outside school for a range of purposes and believe that we have a duty as a school to support pupils and their caregivers in learning how to evaluate internet information and how to take care of their own safety and security.

How does Internet Use Benefit Education?

- access to world-wide educational resources
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management
- exchange of curriculum and administration data with the Local Authority and DFE; access to learning wherever and whenever convenient.

How can internet Use Enhance Learning?

- The school internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils. This filtering is provided by North Tyneside Local Authority.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff will be expected to guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted internet access.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised internet access.
- Parents will be asked to sign and return a pupil 'Acceptable ICT Use Agreement' after discussing it with their child as appropriate.
- Any individuals requiring internet access while at Wellfield will read and sign the 'Acceptable ICT Use Agreement' before using school ICT resources.
- Staff should not access the internet for personal use during formal teaching time. Staff may access the internet for personal use in the staffroom during break and lunchtimes. Staff may access the internet for personal use in the classroom after 3.30.

World Wide Web Protocol

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Senior Leadership Team via the e-safety coordinator or computer technician.
- School will ensure that the use of internet derived materials by pupils and staff complies with copyright law.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- Pupils will be taught to use search engines appropriately for their age.

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

School Gateway

- Parents are contacted using School Gateway who comply with all e-Safety and Data Protection guidelines. Mobile numbers and email addresses are collected from SIMS.net where parents have given permission.

Use of Email

- Pupils may only use e-mail accounts provided by the school.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- Within school, children are only permitted to access their school-provided email address which is not to be used to register for social media accounts.
- E-mail sent to external organisations should be written carefully and, where appropriate, authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters and virals is not permitted. Adults and pupils are asked not to open emails from suspicious / unfamiliar sources.
- Staff should not use personal email accounts during formal teaching time. Staff may access their personal email account in the staffroom during break and lunchtimes. Staff may access their personal emails in the classroom after 3.30pm.

Social Networking

- For the purposes of this policy, social networking can be defined as:

> *"Web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system."*

- Examples would include Facebook, Twitter, LinkedIn, Snapchat and Instagram.
- The school will control access to social media and social networking sites while on-site. Pupils are not permitted to access social media. Staff are permitted to access Twitter for professional use.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address,

mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.

- Pupils will be advised about sensible use of social network space.

- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.

- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.

- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.

- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful, defamatory or reflect negatively on the professionalism of themselves, colleagues or have the potential to bring the school into disrepute.

- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.

- Staff should refer to the school in online publishing spaces only in a positive and professional manner. They should not refer to children or other staff by name online.

- Staff may interact with parents in social media spaces but must ensure that these interactions are professional at all times. They should be acknowledged with the Head Teacher where there may be implications for the adult's position within school. Staff should not using social networks to connect with pupils on the school role.

- All staff, particularly those new to the school should review their social networking sites when they join the school to ensure information publicly available about them is accurate and appropriate.

- All staff have a responsibility to report any unsuitable material of a safeguarding nature or contact between staff and pupils in social networking spaces to the Head Teacher.

Filtering

The school will work in partnership with the network manager and Internet Service Provider to ensure filtering systems are as effective as possible.

- The school's broadband access will include filtering through Smoothwall which is provided by North Tyneside Local Authority.

- The school will have system in place to make changes to the filter, including deciding who is responsible for authorising changes. Requests for changes are made to North Tyneside Local Authority.

- The school will work with the network manager to review filtering

- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.

- If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.

- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.

- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.

- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, local Police or CEOP

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use Policy.

Use of Mobile Devices

- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.

- Staff mobile phones and personal devices will be switched off during formal school time. Mobiles may be kept in classrooms and used in emergency situations. Staff may use their mobile phone during break and lunchtimes in the staffroom or office. Mobile phones may be used in the classroom after 3.30pm.

- Visitors to school will be required to turn their mobile phone off when entering the building. In exceptional circumstances visitors may use their mobile phone while in school.

- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

- Staff are not permitted to use their own personal phones or devices to make phone calls to contact children, young people and their families within or outside of the setting in a professional capacity. Staff may use their phone for responding to emails.

- Staff will use a school landline phone where contact with pupils or parents/carers is required.

- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.

- 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.

- Staff may use a mobile phone at break/dinnertime only and must seek an area of privacy to make the call – such as the staffroom or the school office.

- Any mobile device must be checked for viruses and spam content before being attached to the school network.

- Any use of mobile technology to intimidate, bully, harass or threaten others will be counted as an infringement of network use. This may result in disconnection from the network or legal or civil disciplinary action. Uploading images and sound is only permissible if the subject involved gives permission.

- Staff are permitted to take school-owned iPads home and may install apps for their personal use at home. However, these apps should not be accessed in formal school hours (8.45am – 3.30pm). Staff may also choose to install apps for use in school.

Pupil Use of Mobile Devices

- Pupils should only bring their mobile devices to school where strictly necessary. These should be switched off and kept in lockers throughout the school day.

- The school will have a clear protocol for dealing with illegal content on a pupil owned device. The device should be isolated and the police contacted to help preserve evidence. It should not be further investigated by the school.

- The school will have a system for dealing with inappropriate content on pupil owned devices. Where inappropriate content is found on pupil owned devices the school will confiscate the device and contact parents or carers to discuss.

- If a pupil is found to have a mobile phone in school outside of their locker, it will be removed and placed in the school office for collection at home time.

- School staff may confiscate a phone or device if they believe it is being used to contravene any school policy. The phone or device might be searched by the Senior Leadership team with the consent of the parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.

- Wellfield Middle School cannot be held liable for the loss, damage or theft of personal devices brought to school by children.

- iPads leased through Wellfield's leasing scheme must be kept in line with the terms and conditions set out in the lease and insurance agreements. iPads not leased through Wellfield are not covered by the same insurance policy.

- Children who have access to iPads in school are expected to use them in line with the guidelines set out in their device agreements. These vary depending on whether the iPad is leased, school owned or a personal device brought from home.

Cyberbullying

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" (DCSF, 2007).

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

- All incidents of cyberbullying reported to the school will be recorded using the e-Safety log.

- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.

- Sanctions for those involved in cyberbullying may include:

    - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
    - Internet access may be suspended at school for the user for a period of time.
    - Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying or behaviour policy.
    - Parent/carers of pupils will be informed.
    - The Police will be contacted if a criminal offence is suspected.

Laptops

Laptops for teachers are the property of the school and should be treated like any other school computer.

- The user is responsible for ensuring the privacy and security of data held on any laptop and for ensuring the integrity of such data by keeping antivirus software up to date, as a minimum.

- The laptop should not be used by third parties, by family members or be used for anything other than professional purposes. It should not be loaned out to third parties. It should be kept in a secure location at all times, whether on or off the school site.

- Connection of the laptop to the Internet makes it highly susceptible to interference from outside and this should be borne in mind when using it to browse the web. Laptops containing sensitive pupil data can easily be compromised by connection to any network, but particularly to the internet, and this data could be procured by any third party via an internet connection or perhaps a home wireless network.

- School laptops should not be connected to a third party wireless broadband connection without that party's knowledge and/or permission.

- Laptops brought into school for repair by technicians will be subject to scrutiny if found to contain any virus or suspicious software or document, including dubious images. Any unsuitable content or usage discovered will be reported to the Head Teacher in the first instance.

- Peer to peer (P2P) software must not be installed on any laptop.

- The school reserves the right to audit any school laptop on demand and report any findings related to misuse e.g. pornography or illegal software, to the relevant authority.

- Staff who terminate their employment or are on long term sick leave should return their laptop to the School ensuring that any personal data has been backed up and/or removed

Protecting Computers from Theft

- The e-Safety coordinator and IT technician will investigate the cost of security marking all school ICT equipment.

- Teacher in charge checks equipment at the end of each lesson and makes sure users are logged off and equipment shut down.

Published Content and the School Web Site

The contact details on the school website will be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.

The head teacher and IT technician will take overall editorial responsibility and ensure that content is accurate and appropriate. All school staff are expected to contribute to the development / upkeep of the website as appropriate. Web content management system (CMS) is provided by PrimarySite.

Publishing Pupils' Images and Work

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.
- Pupils work can only be published with their permission or the parents.
- Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.

Information System Security

- School ICT systems capacity and security will be reviewed regularly by the curriculum committee.
- Virus protection will be installed and updated regularly by the network manager
- Security strategies will be discussed with the governing body, network manager and the Head Teacher.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and will report as necessary to the Head Teacher.

Responding to Incidents of Concern

Internet technologies and electronic communications provide children and young people with exciting opportunities to broaden their learning experiences and develop creativity in and out of school. However it is also important to consider the risks associated with the way these technologies can be used.

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.).

- This will take the form of an e-Safety breach log which will be completed by the person present at the time of the breach. These will be kept in the Shared drive. A hard copy will also be placed in the e-Safety folder and an electronic copy emailed to the e-Safety coordinator who can then escalate as appropriate.

- The e-Safety Coordinators will record all reported incidents and actions taken in any other relevant areas e.g. Bullying or Child Protection log.

- The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving child protection concerns, which will then be escalated appropriately.

- The school will manage e-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.

- The school will inform parents/carers of any incidents of concerns as and when required.

- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or e-Safety officer and escalate the concern to the Police.

Handling E-Safety Complaints

- Complaints of Internet misuse by pupils will be dealt with by the Computing Subject Leader and the Head Teacher.
- Any complaint about staff misuse must be referred directly to the Head Teacher.
- Complaints of a child protection nature must be always dealt with in accordance with school child protection procedures.
- Pupils and parents/carers will be informed of the complaints procedure.
- In the event of misuse discussions will be held with the local Police Authority to establish procedures for handling potentially illegal issues
- An Internet E-safety Breach log will be held in school to record any incidents and any actions taken as a result. This will be kept as an electronic copy in DriveStorage. A copy should also be emailed to the computing coordinator and Designated Child Protection Officer.

Communication of Policy

Pupils

- Pupils will be informed that Internet use will be monitored.

- Pupil instruction regarding responsible and safe use will precede Internet access.

- An e–Safety module will be included in the Be Spirited or Computing programmes covering both safe school and home use.

- e-Safety rules or copies of the student Acceptable Use Policy will be posted in all rooms with Internet access.

- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas in relation to the acceptable use policies.

Staff

- The e–Safety Policy will be formally provided to and discussed with all members of staff.

- To protect all staff and pupils, the school will implement Acceptable Use Policies.

- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.

- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could 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.

Parents / Carers

- Parents' attention will be drawn to the school e–Safety Policy in newsletters, the school prospectus and on the school website.

- A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e–Safety at other attended events e.g. parent evenings and sports days.

- Parents will be requested to read and sign the school Acceptable Use Policy for pupils and discuss its implications with their children.

- Information and guidance for parents on e–Safety will be made available to parents I a variety of formats.

- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.

E-Safety Rules

These e-safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network access or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and internet use must be appropriate. Within formal school hours all internet use must be for an educational purpose.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as e-mail could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Staff should not refer to the school, its pupils or members of staff on social media or in personal publishing space e.g. blogs online.
- Use for personal financial gain, gambling, political activity, advertising or unspecified illegal purposes is not permitted.

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

Appendices

WELLFIELD MIDDLE SCHOOL

ACCEPTABLE INTERNET AND MOBILE DEVICE USE STATEMENT FOR ALL SCHOOL STAFF

The computer system is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school has an Internet Access Policy drawn up to protect all parties - the pupils, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

- Access should only be made via the authorised account and password that should not be made available to any other person.
- The security of the ICT system must not be compromised.
- Sites and materials accessed must be appropriate to work in school. Users will recognise materials that are inappropriate and should expect to have their access removed.
- There may be occasions when a teacher may have photos/videos of children on school-owned cameras for educational reasons.
- Images and videos should be stored in the "Shared" area of the school network. Staff may have photos of current pupils in their personal workspace but these must be transferred to the Staff Confidential area or deleted ASAP. Of course, it is expected that such photographs and videos are only used for educational purposes.
- All confidential data including photographs, tracking data and reports should be stored only on an encrypted device when leaving the site. It is expected that this information is only saved encrypted memory pens or school-owned laptops with up-to-date encryption software.
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received.
- The same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded.
- Posting anonymous messages and forwarding chain letters is forbidden.
- Copyright of materials and intellectual property rights must be respected.
- All Internet use should be appropriate to staff professional activity or to student's education. Please note that:-
  - ➢ The school's ICT system may be used for appropriate private purposes outside of school hours.
  - ➢ Use for personal financial gain, gambling, political purposes, advertising or accessing social networks is forbidden.
  - ➢ Closed discussion groups can be useful but the use of public chat rooms is not allowed.
- Staff should not refer to the school, its pupils or members of staff on social media or in personal publishing space e.g. blogs online.
- Staff may interact with parents in social media spaces but must ensure that these interactions are professional at all times.

- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden
- Staff mobile phones and personal devices will be switched off during formal teaching time.
- Personal electronic devices of all kinds that are brought in to school are the responsibility of the user.
- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Any mobile device must be checked for viruses and spam content before being attached to the school network.
- 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.
- Staff may use a mobile phone at break/dinnertime only and must seek an area of privacy to make the call – such as the staffroom or the school office.
- Staff will use a school landline phone where contact with pupils or parents/carers is required.
- Staff will ensure that they lock their computer screen when leaving this unattended.

Members of staff are reminded that they should not deliberately seek out inappropriate / offensive materials on the Internet **and** that they are subject to the LA's recommended disciplinary procedures should they do so.

Staff should sign a copy of this Acceptable Internet Use Statement and return it to the e-Safety coordinator.

Full name _____ Post _____

Signed _____ Date _____

Wellfield Middle School

CONSENT FORM - Responsible Internet Use

Please complete, sign and return to the school as soon as possible.

Pupil's Agreement

I have read and understand the Wellfield Middle School *Using the Internet Policy* and the *Rules for Responsible Internet Use*. I will use the computer system and internet in a responsible way and obey these rules at all times.

Pupil's signature: **Date:**

Please print name:

Parent/Carer's Consent for Internet Access

I have read and understand the Wellfield Middle School *Using the Internet Policy* and the *Rules for Responsible Internet Use* and give permission for my son / daughter to access the internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the internet. I agree that the school is not liable for any damages arising from use of the internet facilities.

Parent/Carer signature: **Date:**

Using the Internet

As a School we will…

- Make pupils aware of the rules and their responsibilities
- Ensure that, wherever possible, websites have been monitored prior to them being used with pupils
- Teach a programme of digital literacy across the school
- Make pupils aware of their responsibility for the communications they send
- Ensure that an appropriate level of Internet filtering is provided to minimise the possibility of accessing inappropriate content
- Monitor pupil usage of the Internet, where necessary
- Ensure that if photographs of pupils are published on the Internet, they are not annotated with their full names or other personal information (such as address and/or phone number)
- Provide appropriate sanctions for pupils who intentionally break the rules of this policy

As a parent, I will…

- Ensure that my child/children understand the importance of following the school's rules for using the Internet

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of E-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

Rules for Responsible Internet Use

The school has installed computers and Internet access to help our learning.

These rules will keep everyone safe and help us be fair to others.

- I will only use my own login.
- If I have been given a password I will keep this a secret.
- I will not access other people's computer account or their work.
- I will use the computers only for schoolwork and homework.
- I will not bring memory sticks into school.
- I will only use websites which my teacher has given me permission to go on.
- When I am using a computer, I will always be polite and sensible.
- I will not give my full name, home address, e-mail address or phone number, or arrange to meet someone, unless my parent, carer or teacher has given permission.
- I will tell a teacher if I see something inappropriate or that makes me unhappy.
- I understand that the school can check my computer files and the Internet sites I visit.
- Be aware that information on an Internet web site may be inaccurate or biased.

Think then click!

E-safety incident	Outline :					
Name of member of staff (Discovering the incident)			Date			
Child(ren) involved. (or other adults if no children involved)			Time			
Device(s), Websites, Usernames..					*Note:- If there is a possibility of legal action the device should be disconnected and powered down. Do not investigate device as this will damage / remove any evidence. Obtain Police advice.*	
Nature of incident	Accidental access to inappropriate material	Intentional access to inappropriate material	Creating / Distributing inappropriate Images	Cyber Bullying	Grooming	Other
Details						
The event occurred Location	During a lesson	In unsupervised time	Outside school hours			

Does the event warrant direct Police involvement (Yes if…)	Grooming	Violent image(s)	Pornographic image(s)	Illegal Images	Blackmail	Other criminal activity
Police Involvement	Yes/No	Date & Time	Contact			
LADO Involvement	Yes/No	Date & Time	Contact			

Head Teacher/Deputy Head / Safguarding Contact					
(Staff)	Contact made with SGSS / Personnel	Recommended action	Action applied	Chair of Govs contacted	
Other Children	Contacted Parents (names)			Date	Time
	Interviewed Parents/Carers Name / Date / Time		Other Interviews Name / Date / Time		Append notes of interviews)
Potential Technical Changes					Completed
Potential Teaching Changes					Completed

Wellfield Middle School

CONSENT FORM – Digital Media Use

Parent/Carer's Consent for Web Publication of Work and Photographs by Wellfield Middle School

I **agree/do not agree* that, if selected, my son's/daughter's work may be published on the school's website.

I **agree/do not agree* that photographs that include my son/daughter may be published in line with the *Digital Media Use* policy.

Parent/Carer's Signature: **Date:**

Parent/Carer's Consent for use of photographs by 3rd parties

I **agree/do not agree* that my child's photograph may be used by 3rd parties, in relation to school activities, both in print media and online, e.g. local journalists at a school event, other schools involved in events such as sporting competitions, drama productions etc. I understand that Wellfield Middle School does not control the use of these photographs and they may not be subject to the guidelines set out in the *Digital Media Use* policy.

Parent/Carer's Signature: **Date:**

Please print name:

Please delete as appropriate

Digital Media Use

The Senior Leadership team have discussed how photographs and videos are used to record events and celebrate achievements at Wellfield Middle School. There are two types of situations where photographs are taken:

a) staff and pupils taking photographs of work being undertaken, school trips, visits, sporting fixtures and special events
b) public situations where the school allows parents and others to take videos and photographs (including local newspapers)

Sadly, we have to take care that any images or photographs taken in school are never misused and reduce the risk of this occurring whenever possible whilst, at the same time, keeping a sensible balance.

Individual pupils will not be named or include other data such as home address/telephone numbers.
We will never use images or photographs that may cause offence, embarrassment or distress to the child or their parent/guardian.
We may use the photographs to add to our website or add to school displays.
We will only use images of pupils in suitable dress.
If Wellfield Middle School has any doubts concerning the appropriateness of a photograph or image, we will, of course, contact parents/guardians and gain written consent before its use.
If parents/guardians want to take photographs or videos of special events, please check with a member of staff before the event. Of course, it is expected that such photographs and videos are only to be used for family purposes and will not be sold or distributed.

Having read the above Policy, I do hope that you feel reassured Wellfield Middle School has done all that it can to ensure the safe and proper use of images and photographs.

We would be grateful if you could complete the Consent Form – Digital Media Use. The completion of the form is a one-off requirement at Wellfield Middle School.

Any parent/guardian who wishes to change their position either by withdrawing consent already given or giving consent for the future, must do so in writing, addressed to the Head Teacher.

WELLFIELD MIDDLE SCHOOL

ACCEPTABLE INTERNET AND MOBILE DEVICE USE STATEMENT FOR ALL VOLUNTEERS

The computer system is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school has an Internet Access Policy drawn up to protect all parties - the pupils, the staff, volunteers and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

- Access should only be made via the authorised account and password that should not be made available to any other person.
- The security of the ICT system must not be compromised.
- Sites and materials accessed must be appropriate to work in school. Users will recognise materials that are inappropriate and should expect to have their access removed.
- Visitors to the school should refrain from taking photographs of pupils. Where there is a need for this, it should be done with a school-owned device and supervised by a member of staff.
- Visitors should in no circumstances remove confidential data, such as tracking or reports, from school premises, in either electronic or hard-copy form.
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received.
- The same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded.
- Posting anonymous messages and forwarding chain letters is forbidden.
- Copyright of materials and intellectual property rights must be respected.
- All Internet use should be appropriate to staff professional activity or to student's education. Please note that:-
  - ➢ The school's ICT system may be used for appropriate private purposes outside of school hours.
  - ➢ Use for personal financial gain, gambling, political purposes, advertising or accessing social networks is forbidden.
  - ➢ Closed discussion groups can be useful but the use of public chat rooms is not allowed.
- Staff/volunteers should not refer to the school, its pupils or members of staff on social media or in personal publishing space e.g. blogs online.
- Staff/volunteers may interact with parents in social media spaces but must ensure that these interactions are professional at all times.

- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Designated Child Protection Coordinator.

- I will ensure that any electronic communications with pupils are compatible with my professional role.

- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden
- Staff/volunteers mobile phones and personal devices will be switched off during formal teaching time.
- Personal electronic devices of all kinds that are brought in to school are the responsibility of the user.
- Staff/volunteers are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Any mobile device must be checked for viruses and spam content before being attached to the school network.
- Staff/volunteers 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.
- Staff/volunteers may use a mobile phone at break/dinnertime only and must seek an area of privacy to make the call – such as the staffroom or the school office.
- Staff/volunteers will use a school landline phone where contact with pupils or parents/carers is required.
- Staff/volunteers will ensure that they lock their computer screen when leaving this unattended.

Members of staff/volunteers are reminded that they should not deliberately seek out inappropriate / offensive materials on the Internet **and** that they are subject to the LA's recommended disciplinary procedures should they do so.

Volunteers should sign a copy of this Acceptable Internet Use Statement and return it to the school office.

Full name _____ Post _____

Signed _____ Date _____