Wellfield Middle School

Online Safety Policy

Our Online Safety Policy has been written by Wellfield Middle School building on the North Tyneside Online Safety draft policy and government guidance. It has been agreed by senior management and approved by governors.

Our Online Safety Policy has been written by the computing subject leader and computer technician and seeks to incorporate the current government guidance and nationally recognised best practice. It has been agreed by the SLT and is pending approval by the school governing body in September 2020

The Online Safety Policy for Wellfield Middle School will be reviewed annually. This policy will next be reviewed in September 2021

The Online Safety Policy was revised by: Bev Stephenson and Duncan Turner

It was approved by the Governors on:

The next review date is : September 2021

Contents

Policy Aims

- The purpose of the online safety policy is to:
    - Safeguard and protect all members of the Wellfield Middle 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 model positive behaviour online and to manage professional standards and practices when using technology;
    - Enable learners to be empowered to build resilience and to develop strategies to manage and respond to risk online;
    - Identify clear procedures to use when responding to online safety concerns.
- This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as “staff” in this policy), as well as learners, parents and carers.
- Wellfield Middle School 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.

Links with other policies and practices

This policy links with several other policies, practices and action plans including:

- Anti-bullying policy;
- Acceptable Use Policies (AUP);
- Behaviour policy;
- Child protection policy;
- Confidentiality policy;
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE);
- Data security;
- Image use policy;
- Mobile phone and social media policies;[DT1]
- GDPR / Information Governance procedures policy.

Roles and Responsibilities

Wellfield Middle School has an appointed Online Safety Coordinator (Duncan Turner, computing coordinator). The Designated Safeguarding Lead is Susan Winter (Head Teacher) and the Deputy Designated Safeguarding Leads are Caroline Kemp (Deputy Head Teacher), Jenny Hawkridge (Assistant Head Teacher) and Susan Pattinson (Teaching Assistant). The on-site computer technician is Bev Stephenson.

Our online safety coordinator's responsibilities are to ensure:

- They keep up to date with online safety issues and guidance through liaison with the Local Authority, and through organisations including The Child Exploitation and Online Protection command (CEOP);
- The senior leadership and Governors are updated as in line with current Government Guidelines;
- That the policy is implemented and that compliance with the policy is actively monitored;
- All staff are aware of reporting procedures and requirements should an online safety incident occur;
- The online safety Incident Log is appropriately maintained and regularly reviewed;
- Providing or arranging online safety advice/training for staff, parents/carers and governors;
- Close liaison with the school's Designated Safeguarding Lead to ensure a coordinated approach across relevant safeguarding areas.

Governors need to have an overview of online safety issues and strategies at Wellfield Middle School. The computing link governor should be aware of local and national guidance regarding online safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours, in their classrooms and when using technology, and following school online safety procedures. Central to this is fostering a culture where pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the school's policy.

All staff and visiting adults with access to the school’s Internet should sign the Acceptable Use Policy

Staff are updated about online safety matters at least annually.

Teaching and learning

Why the Internet and digital communications are important

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

The Technologies

New technologies are enhancing communication and the sharing of information and are constantly evolving. Current and emerging technologies used in school include but are not limited to:

- e-mail;
- Voice over IP (VOIP);
- Instant messaging, often using simple web cams;
- Blogs;
- Podcasting;
- Video broadcasting sites;
- Music download sites;
- Devices with camera and video functionality;
- iPads, tablets and eReaders

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- communication and collaboration with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the LA and DfE;
- access to learning wherever and whenever convenient.

Internet use will enhance learning:

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils;
- Pupils will be taught what Internet use is and what is not acceptable and given clear objectives for Internet use;
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation;
- Pupils will be shown how to publish responsibly and present information to a wider audience.

Pupils will be taught how to evaluate Internet content

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils will be taught the importance of cross-checking information before accepting its accuracy. Pupils will be taught how to report unpleasant Internet content in school and at home or online e.g. using the CEOP Report Abuse icon.

Remote Learning

During the recent period of long-term closure, and in the event of possible future school closures, Wellfield Middle will continue to provide education and support to our pupils using remote learning tools.

Content will be set for each year group in line with a timetable which has been agreed by staff and shared with children and parents. In most cases, this will consist of three lessons per day, unless alternative agreements are in place with individual families.

All work will be shared through Google Classroom and should be returned either through this platform or uploaded to Seesaw. Staff will provide clear instructions and deadlines for the completion of work and should be available through remote communication (email) to deal with queries throughout the working day.

At all times, communication should put the well-being of the children first and be supportive and encouraging. This should take place only through secure, school-approved technologies (Google Classroom, Google Meet, Wellfield email addresses). When using Google Meet, staff should ensure they are the last person to leave the meeting to ensure that pupils do not have unsupervised access. In line with good safeguarding practice, staff should avoid holding a Google Meet in a situation in which they are left 1:1 with an individual pupil.

Infrastructure and technology

Network Passwords

All users of the school network have a secure username and password.

All staff and pupils are reminded of the importance of keeping passwords secure. If a pupil, or member of staff, believes that someone other than themselves has become aware of their password, they are to report to the online safety coordinator or ICT Technician and their password will be changed.

Pupil Internet Access

Pupils are given guidance about available, appropriate materials to use and understand that their Internet use is monitored and can be traced to individual users. This is managed through NetSupport, which identifies and informs the ICT technician of inappropriate search terms and takes a screenshot of the PC / iPad screen in question.

Software/hardware

All software and apps have been purchased, and are legally owned by, the school. The dates of appropriate licenses are recorded and kept with the secure passwords in the school office.

Pupil iPad devices are provided on a 1:1 basis in one of three ways: bring-your-own-device (BYOD), a lease scheme or school-owned. For further information on the different ways in which these are managed, please see the Acceptable Use Policy..

- The school technician loads any new software onto the schools network.

- The school maintains the licences and arranges to have any software removed when licensing has expired.

- Staff can be provided with a school-owned laptop which should only be used for work related to school
- Staff may access their work emails via personal devices but should not use their personal device to take pictures of children.
- Staff iPads should not be used to access personal email or social media accounts.
- 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).

Web filtering and virus protection

Virus protection is purchased for the network and all school computers. Regular scans should be performed by staff on devices that are not connected to the Network.

Any device suspected or found to contain any virus or malware must be immediately turned off and removed from the network. The ICT coordinator must then be informed so appropriate technical support can be sought.

The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Internet filtering is provided by Fortinet, which is purchased from BlueCube and supported through Engie. Fortinet has sophisticated text, image and URL scanning for users accessing and attempting to access inappropriate content. Filtered content is classified by the following categories:

- abuse,
- adult content,
- bullying,
- criminal activity,
- radicalisation,
- sustance abuse,
- suicide.

All breaches are logged by Fortinet and can be traced back to identify school, machine, time and date. Logs of misuse can be obtained through Fortinet upon request.

While strong filters are in place, no filtering is 100% effective and so staff must remain vigilant for inappropriate content when using the internet. If anything inappropriate is found staff should turn off the screen of the machine and remove it from use. They should then (if possible) screen capture the website and report it to the IT technician so it can be reviewed and blocked if necessary.

Staff may also request for websites to be unblocked if they believe they are appropriate for educational purposes by contacting the IT technician.

Staff are permitted to use an amended version of the filtering system that allows access to Youtube and Facebook. This has been agreed by senior management in school but must only be used on staff devices. Staff must still exercise caution when using sites like Youtube and pre-plan videos to be shown and avoid 'live searches' for videos in class where possible. This can reduce the risk of students being exposed to unsavoury comments below a video.

Students will have access to YouTube via Restricted Mode which will filter out mature or inappropriate content. They will also be able to access videos pre-approved by staff.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

School ICT systems security and security strategies will be reviewed internally and may be reviewed and discussed with the Local Authority.

Any material that the school believes is illegal must be reported to appropriate agencies such as the Internet Watch Foundation (IWF) or CEOP: Child Exploitation and Online Protection command.

Managing the network and technical support

The server and cabling is located in a lockable office and its physical access is restricted. Only staff are permitted to access this area. Children assisting staff must be accompanied at all times. The network is managed by Bev Stephenson with support from the Local Authority.

The network is monitored via the council.

Requests for technical support can be made to bev.stephenson@wellfieldmiddleschool.org.uk.

Use of Technology

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

Mobile Devices

This section is intended to reflect rules around use of mobile phones and smart watches and iPads but may be extended to include any items that may be reasonably considered as mobile, electronic devices.

Pupil Use

Students should only bring their personal mobile phones to school with them where strictly necessary. They should be switched off (not simply on silent) upon reaching the school grounds and remain in a bag, inside the pupil's locker throughout the day. They should not be used anywhere within the school grounds. Under exceptional circumstances, staff may grant students permission to use their mobile phone, for example to contact a parent or carer following return from a trip. It is now commonplace for a large number of students to own a 'smartwatch'. While Wellfield recognises the advantages of such technology, those which are data-enabled and can send and receive messages may present a safeguarding risk and are not permitted to be worn.

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 the end of the school day.

School staff may confiscate a phone or device if they believe it is being used to contravene any school policy. Under government guidelines, the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate. 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.

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 may vary depending on whether the iPad is leased, school owned or a personal device brought from home.

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

Staff and Visitor Use

Our school allows personal mobile phones to be used in school by staff and visitors, however they are not to be used within the classroom or when pupils are present. Phones should be turned off or on silent during lessons. We regard it acceptable for staff to use personal mobile phones for school activities e.g. school trips, when communication with school is necessary. However, personal devices should not be used to take photographs of pupils.

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.

When contacting parents / carers, staff should use a school landline phone when in the building. In exceptional circumstances, such as those during the recent Covid-19 pandemic, staff may use their personal mobile devices but should withhold their number from parents and carers. Staff should not contact pupils directly via a voice or video call.

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.

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.

Digital Communication

Email

Email provision for staff and students is provided by Google for Education.

Staff and pupils may only use approved email accounts on the school system.

All email is filtered. Email content, titles, addresses and attachments are scanned for questionable content, which is maintained by the IT Technician on behalf of Wellfield Middle School. Mail that breaches the guidelines for security or appropriateness is blocked from reaching its intended destination and placed into a quarantine folder. Quarantine items are checked by the IT Technician on a regular basis and reports are made to headteachers where anything of concern is captured.

As pupils join the school, they are added to our schools SIMS database and have an account created on their behalf.

Staff must create and maintain passwords in accordance with the Google requirements (minimum of 8 character length).

Staff must create and maintain passwords in accordance with the Google requirements (minimum of 8 character length). There is no requirement to change them on any timescale but talking about good passwords is something that will be covered as part of online safety lessons as they progress through school.

- Pupils must immediately tell a teacher if they receive offensive email;
- In email communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone
- Incoming email should be treated as suspicious and attachments not opened unless the sender is known;
- Pupils should not send emails outside of the Wellfield Middle School domain without prior, specific permission from a member of staff
- The sending of abusive or inappropriate email messages is forbidden;
- Electronic mail should only be used in the course of work as a student and only using the authorised logins provided by the school;

- Users must never use electronic mail to send or forward chain letters or any material which may contravene school policies (e.g. jokes, pictures of a racist, homophobic or sexist nature);

- Users must only copy messages (i.e. cc or bcc) to people where it is of direct relevance.

Staff use

- Staff are expected to check their email mailboxes regularly. They should ensure that notifications or message previews are not visible to students at any time.

- The use of personal web based email in school is forbidden to minimise the risk of unsuitable materials and viruses from external email accounts.

- All users are aware that email is covered by GDPR, meaning that safe practice should be followed in respect of record keeping and security.

- All users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.

- All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

Social Networks for school communications

School communication

- The school will control access to social networking sites for school communication;

- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for pupils and app age limits should be taken into account;

- Permissions will be sought before any content relating to a child is posted on a social media site - also refer to the use of digital media and the website section of this document;

Inline with this policy:

- Staff are expected to manage their digital identity and portray themselves in a positive, professional and appropriate manner when posting or sharing content online;
- Staff should have privacy settings in place and should check and review these on a regular basis;
- Staff should not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any personal blogs or websites;
- Staff should not add pupils as “Friends” on any Social Network site;
- Staff should never post on behalf of, or refer to the school, pupils or parents on any social networking site, unless it is from the school’s official accounts and in a professional and appropriate manner
- Users of social media should consider copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing;
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Instant Messaging:

Instant Messaging, e.g. WhatsApp, Facebook Messenger etc. provide an opportunity to communicate in real time using text, sound and video. It is not appropriate to use these tools in school.

Gmail provides its own filtered instant messaging ‘chat’ and ‘video chat’ service, Google Meet, which should be the only messaging service used in school, and then only used by students with adult permission and supervision.

Published content and the school website

The school website is (https://www.wellfieldmiddleschool.org.uk/). It provides key information to the public about the school, promotes the school and celebrates pupils’ work.

Staff or pupil personal contact information will not be published.

The following members of staff have administrative rights to edit our school website:

- Bev Stephenson
- Diane Hill
- Duncan Turner
- James Matthewson
- Susan Winter

The headteacher will take overall editorial responsibility and will ensure that content is accurate and appropriate.

Our website is fully compliant with Government and Ofsted requirements for schools maintained by a local authority.

Video conferencing

Any use of video conferencing/video chats must only take place with the permission of a member of the senior leadership team (SLT). All use of video conferencing should take place through Google Meet in Google Classroom. An adult must always be aware that a video conference/chat is taking place. Children should be consulted and adults would need to consent as well as the parents of all children involved.

Children must be educated about safe, appropriate and acceptable use of video conferencing technologies, considering the following points:

- how, when and why they make use of it;
- ensuring an appropriate adult knows they are using it;
- never accepting a chat request from someone they do not know;
- reporting anything they find upsetting or inappropriate in a video chat to a trusted adult;
- protecting their personal information when using it. This may include not just what they say in a ‘chat’, but even the objects in the room around them which may inadvertently give away personal information they don’t wish to share.

Use of digital media

In our school we are aware of the issues surrounding the use of digital media online. All members of our school are required to follow the school's guidance below.

- All staff and pupils instructed that full names and personal details should not be used on any digital media, particularly in association with photographs;
- We ask all parents/carers to provide written permission stating whether or not they can have their photograph taken and used within school or on the school website;
- Pupil image file names will not refer to the pupil by their full name;
- All staff are instructed of the risks associated with publishing images, particularly in relation to use of personal Social Network sites;
- Our school ensures that photographs/videos are only stored using school-owned equipment and only for school purposes;
- We do not allow staff to store digital content on personal equipment;
- When taking photographs/video, staff ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted;
- Staff, parents/carers and pupils are made aware of the dangers of publishing images and videos of pupils or adults on Social Network sites or websites without consent of the persons involved.
- Parents are clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories;
- Staff sign an AUP informing them of the guidelines for safe practice relating to the use of digital media, as outlined in the schools' policy. These are monitored by our online safety coordinator and SLT.

Protecting personal data

Personal data will be recorded, processed, transferred and made available inline with GDPR.

Policy Decisions

Authorising Internet access

- All staff who use the school Internet or technology must read and sign the Acceptable Use Policy before using any school ICT resources;
- School visitors sign to accept the terms of the Visitor Agreement which includes guidelines on use of technology
- All pupils and parents must read and sign the Acceptable Use Policy before using any school ICT resources;
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- This online safety policy will be published on the school website and advice on the safe use of the internet will be provided.

Handling online safety incidents

Our online safety coordinator acts as the first point of contact for any complaint. The Local Authority supplies the following document to suggest appropriate action when dealing with online safety, and in particular social networking related, incidents.

Click here to access - How to deal with an online safety incident involving staff 2019 v3

Assessing risks

The school will take all reasonable precautions to ensure online safety and prevent access to inappropriate material. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school site.

- The school will audit ICT use to establish if the online safety policy is adequate and that the implementation of the policy is appropriate and effective;
- Methods to identify, assess and minimise risks will be reviewed regularly;
- The SLT will ensure that the online safety policy is implemented and compliance with the policy monitored.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Incidents involving pupils

- Incidents of cyberbullying are dealt with in accordance with our bullying and behaviour policy;
- Incidents related to child protection are dealt with in accordance with the school's child protection policy and reported to the Headteacher immediately
- The device where the incident took place (if in school) must be taken out of use until appropriate evidence can be captured to log the incident;
- All staff are made aware of different types of online safety incidents and know that they must report them immediately.
- Once incidents have been reported, a record must be made by the member of staff involved, which will then be filed on CPOMS.
- If necessary the Local Authority will be informed of any misuse and parents will be informed.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.
- Parents and pupils will need to work in partnership with staff to resolve issues.

As with other safeguarding issues, there may be occasions when other outside agencies must be contacted. Incidents of a criminal nature; i.e. threatening, intimidation or harassment then may then involve contact with the police for further advice (at the discretion of the headteacher).

Parents and pupils are given information about infringements and possible sanctions.
Sanctions for pupils include:

- informing parents or carers;
- removal of Internet or computer access for a period of time.
- referral to LA / Police.

Incidents involving staff

- Any incident involving staff misuse must be referred immediately to the Headteacher.

If a member of staff suspects that they are in breach of this policy whilst acting in good faith they must notify the Headteacher or nominated online safety coordinator IMMEDIATELY so that action can be taken to prevent or minimise damage.

Any authorised user who commits a breach of any school policy as a result of unauthorised use of electronic media may face disciplinary procedures. If the school discovers that a member of staff has committed a criminal offence or has been a party to the commission of one as a result of unauthorised use of electronic media the police will be contacted immediately. The school will in no way indemnify a member of staff who has incurred any liability as a result of unauthorised use of electronic media. The school will seek financial redress from an authorised user whose misuse of electronic media causes the school to suffer a loss.

Incidents involving other adults (e.g. parents)

- Any incident affecting the school but involving other adults out of school must be referred immediately to the Headteacher;
- Where possible, evidence should be collected immediately and individuals concerned may be contacted by the Headteacher to discuss the incident;
- If necessary the Local Authority will be informed of any misuse;
- Incidents of a criminal nature; i.e. threatening, intimidation or harassment then may involve the police for further advice (at the discretion of the Headteacher).

Introducing the online safety policy to pupils

- Online safety rules will be posted in all rooms where computers are used and discussed with pupils regularly;
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up;
- A programme of training in online safety will be used with staff and students.

Online safety training will be embedded within the computing scheme of work and the Personal Social and Health Education (PSHE) curriculum. Key resources to support this are Project Evolve from South West Grid for Learning and the UK Safer Internet Centre, and Common Sense Education's Digital Citizenship curriculum.

Staff and the online safety policy

- All staff will be given the online safety policy and its importance explained;
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user;
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and follow clear procedures for reporting issues;
- Staff will always use a safe search engine when accessing the web with pupils;
- The school will liaise with the LA as part of the ICT SLA to provide effective support to staff.

Enlisting parents' and carers' support

- Parents and carers will be reminded of the acceptable use policy for children at the start of each academic year;
- Throughout the year parents and carers will be reminded about the online safety policy in newsletters, through Twitter and the school website;
- Wellfield Middle School will maintain a list of online safety resources for parents/carers;
- The school will liaise with the LA as part of the ICT SLA to provide effective support to parents and carers.

Standards and inspection

- Staff will regularly remind children of online safety rules and any incidents that occur will be reported to the online safety coordinator;
- Each incident that takes place will be reviewed by the online safety coordinator or member of SLT and appropriate action will be taken immediately;
- Incidents will be analysed to see if there is a recurring pattern e.g. specific days, times, classes, individual children etc.;
- If a pattern emerges they will be addressed through targeted interventions with the appropriate groups;
- All stakeholders are informed of changes to policy and practice via newsletters, meetings and training sessions;
- AUPs are reviewed annually and updated to include new technologies, when necessary.

Prevent Duty

As of 1 July 2015, all schools, and registered early years and childcare providers are subject to section 26 of the Counter-Terrorism and Security Act 2015, also known as the Prevent duty. This states that they must have ‘due regard to the need to prevent people from being drawn into terrorism’. Issues relating to this are covered in the school safeguarding policies, but school is also aware of the risks that digital technologies pose for young people in being exposed to radicalisation and extremism. Much of this policy covers the ways in which school strives to keep young people safe and minimise risks they face while they engage with technology.

Leavers Policy

What to Do When a Teacher/ Staff member Leaves

The purpose of this section is to:

- Help ensure that school's data and resources remain secure as personnel leave the organisation
- Help reduce the opportunity for misplaced or malicious allegations.

Adults who work in schools may have access to a range of important and sensitive information including images and personal details of colleagues and learners and it is essential that the integrity of the school's systems and files remain intact when colleagues leave the school.

Email – disable password. School technical administrators may need to keep access to the account by forwarding mail to an alternative account. This will help address any ongoing issues, projects that need to be completed, outstanding actions etc.

Network – change access password. Delete files or inspect prior to making them available to other users.

Secure areas – ensure key codes are changed and all keys retrieved.

Portable devices – use of devices such as USB memory pens, which must be encrypted, should be kept to a minimum. Valuable or important documents and information should also be stored in Google Drive for security.

Google Drive – account disabled but not deleted. This will ensure all useful documents can continue to be used by the school. Ownership of necessary documents should be altered as soon as is practical.

Files, programs, data - ensure none are taken away from the school if the copyright is only for the institution.

Images – no teacher can take images of pupils away from school when they cease to be employed by the school.

What to Do When a Pupil Leaves

Network – remove log-in from system. Delete files or inspect prior to making them available to other users.

Google Drive – accounts are removed manually as they leave school. It is not possible to transfer their account ownership to another school.

Staff and Governor - Acceptable Use Policy

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This AUP is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarifications should be discussed with the computing subject leader, IT technician or headteacher.

- I understand that ICT includes a wide range of systems including devices, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone numbers and personal email address, to pupils/parents/carers.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school or accessed remotely.
- I will not install any hardware or software without permission.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Headteacher.

- I will support the school approach to online safety and not deliberately upload or add any images, video, sound or text that could upset or offend any member of the school community

- I will respect copyright and intellectual property rights.

- I will not be involved with any online activities, either within or outside school that may bring the school, staff, pupils or wider members into disrepute. This includes derogatory/inflammatory, offensive, illegal or discriminatory comments made on social network sites, forums and chat rooms.

- I will be an active participant in online safety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.

- I will not use the school system(s) for personal use during working hours.

- I will always consult the headteacher before ordering any goods intended for school use via the internet.

- I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.

- I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.

- I have a duty to protect passwords and personal network logins, and should log off the network or lock the computer when leaving workstations unattended.

- I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.

- I acknowledge that when I am logged on to a school computer, I am responsible for its overall use, including use of the internet.

- I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature ……..…… Date ……...

Full Name ……. Job title……

Student - Acceptable Use Policy

I understand that I must use school systems in a responsible way, to make sure that there is no risk to myself, the school or others.

- I understand that Wellfield will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure and I will not access other people's computer account or their work.
- I will not share personal information about myself or others when online (e.g. names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.).
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.
- I will only use technology at Wellfield for schoolwork and homework.
- I will not take, store or share images of anyone without their and my teacher's permission.
- When I am using a computer, I will always be polite and sensible.
- If I come across damaged or faulty equipment, I will report it to a member of staff.
- I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to keep myself and others safe.
- I understand that I am responsible for my actions, both in and out of school:
- I understand that if my actions in or out of school go against any of the statements in this document Wellfield Middle School can impose school sanctions.

Student Signature

I agree to follow the rules and to support the safe use of ICT throughout the school

Full Name …….. Date ……

Parents/Carers Name …….. Date ……

iPad Acceptable Use Policy

Wellfield Middle School 1-1 iPad Policy – Leased iPads

In order to use a leased iPad on school property the following terms must be agreed with.

I agree:

• The iPad will be 'supervised' by the school; This means that school can monitor the iPad, and install apps remotely. The iPad may not be used in school if the supervision profile is removed (Lightspeed Mobile Management)

• The device should be brought to school fully charged every day. It should be in the provided case with the child's name prominently visible.

• Any apps required in school will be provided by the school and placed on the iPad using our management software. These Apps remain the property of the school and will be removed when the student leaves the school.

• All content on the iPad must be age appropriate, this will be monitored in school.

• The iPad is for personal use and should not be shared.

• Use of iPads during the school day is at the discretion of teachers and staff. Pupils must only use iPads as directed by their teacher. Using the device for personal reasons e.g. contacting parents, should not take place.

• The use of an iPad is not to be a distraction in any way to teachers or pupils.

• Students will not use iPads to record audio or take photographs or video of other students or members of staff without prior permission. Students will not transmit or upload such media without permission.

• Pupils shall not use iPads outside of their classroom unless otherwise directed by their teacher e.g. on school visits or activities.

• Pupils shall make no attempts to circumvent the school's network security and/or filtering policies.

Consequences for Misuse/Disruption (one or more may apply):

• Access to the wireless network will be removed.
• Device taken away for the period.
• Device taken away and kept in the front office until parent picks it up.
• Student is not allowed to use personal devices at school.
• Serious misuse of Internet capable devices is regarded as a serious offence within the School's Behaviour Management Policy and will be dealt with in accordance with this policy.

School Liability Statement Pupils bring their iPads to use at Wellfield Middle School at their own risk. Pupils are expected to act responsibly with regards to their own device. It is their duty to be responsible for the protection of their devices. Leased iPads are insured and details of the policy can be found on our website. http://www.wellfieldmiddleschool.org.uk/ipad-leasing-scheme/

Wellfield Middle School 1-1 iPad Policy - School Owned iPads

Your student will be provided with an individual iPad to use within school hours, in order to use this iPad the following terms must be agreed with :-

I agree:

• The iPads are ‘supervised’ by the school; This means that school can monitor the iPad.

• The device should left in school at all times, the student will be given a location to store and charge the iPad overnight in their classroom.

• Use of iPads during the school day is at the discretion of teachers and staff. Pupils must only use iPads as directed by their teacher. Using the device for personal reasons e.g. contacting parents, should not take place.

• The use of an iPad is not to be a distraction in any way to teachers or pupils.

• iPads must not disrupt class in any way.

• Students will not use iPads to record audio or take photographs or video of other students or members of staff without their permission. Students will not transmit or upload such media without permission.

• Pupils shall not use iPads outside of their classroom unless otherwise directed by their teacher e.g. on school visits or activities.

• Pupils shall make no attempts to circumvent the school’s network security and/or filtering policies.

Consequences for Misuse/Disruption (one or more may apply):

o Access to the wireless network will be removed.

o Device taken away for the period.

o Device taken away and kept in the front office until parent picks it up.

o Student is not allowed to use personal devices at school.

o Serious misuse of Internet capable devices is regarded as a serious offence within the School’s Behaviour Management Policy and will be dealt with in accordance with this policy.

Wellfield Middle School 1-1 iPad Policy – Bring Your Own iPad.

In order to use a personal iPad on school property the following terms must be agreed with.

I agree:

- The iPad will be 'supervised' by the school; The iPad will be cleared of all content, and a supervision profile will be installed on it. iPads will only be able to gain access to the internet in school when they have this profile installed. (Lightspeed Mobile Management)
- The device should be brought to school fully charged every day. It should be in a sturdy case with the child's name prominently visible. We are using STM Dux cases for our leased iPads. We recommend the device is insured.
- The device may only be connected to the internet via WIFI, any iPads that are 3G enabled must have SIM cards removed.
- Any apps required in school will be provided by the school and placed on the iPad using our management software. These Apps remain the property of the school and will be removed when the student leaves the school.
- All content on the iPad must be age appropriate, this will be monitored in school.
- The iPad is for personal use and should not be shared.
- Use of personal iPads during the school day is at the discretion of teachers and staff. Pupils must only use iPads as directed by their teacher. Using the device for personal reasons e.g. contacting parents, should not take place.
- Students will not use iPads to record audio or take photographs or videos of other students or members of staff without prior permission. Students will not transmit or upload such media without permission.
- The use of a personal device is not to be a distraction in any way to teachers or pupils.
- Pupils shall not use personal devices outside of their classroom unless otherwise directed by their teacher e.g. on school visits or activities.
- Pupils shall make no attempts to circumvent the school's network security and/or filtering policies.

Consequences for Misuse/Disruption (one or more may apply):

- Access to the wireless network will be removed.
- Device taken away for the period.
- Device taken away and kept in the front office until parent picks it up.
- Student is not allowed to use personal devices at school.
- Serious misuse of internet capable devices is regarded as a serious offence within the School's Behaviour Management Policy and will be dealt with in accordance with this policy.

School Liability Statement

Pupils bring their iPads to use at Wellfield Middle School at their own risk. Pupils are expected to act responsibly with regards to their own device, keeping it up to date and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices.

I agree to the above policy, and accept that Wellfield Middle School is in no way responsible for:

- Personal iPads that are broken whilst at school or during school-sponsored activities
- Personal iPads that are lost or stolen at school or during school-sponsored activities
- Maintenance or upkeep of any device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues).

Additional Useful Documents

- Sexting in schools and colleges: Responding to incidents and safeguarding young people
- Sexual violence and sexual harassment between children in schools and colleges
- The Prevent duty
- Keeping children safe in education
- What maintained schools must publish online
