Reaching higher by learning and growing together.

LAYFIELD PRIMARY SCHOOL

Computing Policy

February 2018

Review Date: February 2019

Content:

Context

1.1 The School's Information Communication Technology Policy is part of the School Improvement plan and Computing action Plan. It relates to other policies including those for behaviour and for personal, social and health education (PSHE) including citizenship.

1.2 The Computing policy has been written by the Computing subject leader with advice from Local Authority consultants. It will be reviewed on a yearly basis. It has been agreed by the senior management and approved by governors.

Revised: February 2018 by Mr L Barker

To be revised again: February, 2019

A Vision for Computing

2.1 At Layfield:

- That computing is integral to school life.
- That e-safety is at the core of all computing teaching.
- That computing is able to cater for all children's individual needs and is used to support a range of learning styles.
- That pupils are empowered to take control of their own computing learning and are able to extend their learning beyond the classroom through increased access to resources.
- That pupils learning of the whole curriculum is enhanced through the use of a range of technologies.
- That pupils are prepared for the future and the new technology it holds.
- That staff are supported through CPD as they are paramount to success.

2.2 We can achieve this vision by:

- Helping children to develop a range of computing skills which will enable them to make effective use of resources for themselves.
- Encouraging all pupils to have confidence to experiment with new software and apply their developing skills in new contexts.
- Developing an understanding of when computing can give quicker or better results than other methods and also of when it might be inappropriate to use computing.

- Helping children to gain a sense of achievement by developing the patience and persistence to realise their ideas and recognise the possibilities of going wrong without the feeling of a sense of failure.

2.3 Our aims for computing education are to ensure that all pupils:

- Can understand and apply the fundamental principles and concepts of computer science, including abstraction, logic, algorithms and data representation
- Can analyse problems in computational terms, and have repeated practical experience of writing computer programs in order to solve such problems
- Can evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems
- Are responsible, competent, confident and creative users of information and communication technology.

Principles for the use of computing

2.4 Computing education is important because:

- It equips pupils to use computational thinking and creativity to understand and change the world.
- It has deep links with mathematics, science, and design and technology.
- It provides insights into both natural and artificial systems.
- It equips pupils to create programs, systems and a range of content.
- It ensures that pupils become digitally literate at a suitable level for the future workplace and as active participants in a digital world.
- It prepares pupils to participate in a rapidly changing world in which work and leisure are increasingly transformed by access to new technologies.
- It enables children to employ computing to access ideas and experiences from a wide range of people, communities and cultures.
- It increases capability promotes initiative and independent learning and the ability to be selective about its use.

Safeguarding

2.5 Ensuring the safety of pupils and staff is of primary importance. Safeguarding procedures are described throughout this policy and are in place to safeguard all members of the school community. Cyber bullying is taken seriously in our school and so all safeguarding procedures should be followed with regards to the use of electronic devices as outlined below.

Teaching and Learning

National Curriculum

3.1 By its very nature the Computing Curriculum is liable to change frequently. The plan for developing the curriculum and managing changes is outlined in the school's Computing Action Plan which is updated at least once a year by the Computing Subject Leader. It includes proposals for future development of the curriculum, use of resources, staff training needs and long-term replacement of hardware. Not all the required changes can be made in the short term because of the cost and training time involved.

3.2 The delivery of the computing curriculum at Early Years Foundation Stage and Key Stages 1 and 2 will taught through the Purple Mash Whole School Plan. This is available here https://www.purplemash.com/?dm_i=R2J,5E18Q,P1FRO6,KULLT,1#app/schemes_of_work/computing_schemes_of_work/computing_sow_overview

3.3 The implementation of the statements will ensure a continuity and progression of skills, knowledge and understanding across the school by implementing computing skills in meaningful and cross curricular ways.

Foundation Stage

3.3 Nursery and Reception pupils are taught through the EYFS curriculum using 'Development Matters' goals and is assessed using the Early Learning Goals where clear outcomes are found in the section related to Understanding the World (UTW). The work is ongoing throughout the year and is differentiated according to ability.

Cross-curricular Links

3.4 Information Communication Technology has many cross curricular opportunities which teachers are encouraged to make the most of.

3.5 Computing must be presented in practical contexts which will be relevant to the children's experiences. In computing, pupils must have "hands on" experience.

3.6 In Key Stages 1 and 2, computing will be used to support and extend learning throughout the creative curriculum. It will also be used to present and showcase work across the curriculum.

Special Educational Needs

3.9 Pupils with Special Needs have the same computing entitlement as all other pupils and are offered the same curriculum. However, in addition particular aspects of computing are used for:

- Pupils with difficulties in learning, who need to be motivated to practice basic skills regularly and intensively, and thus benefit from the use of programs in which skills practice is predominant

- Pupils of high ability who may be extended through the use of programs which offer challenge and opportunities for investigation.

Assessment and Recording

3.11 On-going assessment has always been an integral part of good practice. It is done in line with the school's assessment policy, through observation of the pupil's work, discussion and the outcome of set tasks. The school is using the same assessment principles as in Literacy, Numeracy and Science and so the children will be given a red (1) if one piece of evidence has been seen, orange (2) if evidence has been seen twice and green (3) if they have fully met the objective.

Children now have a folder within Purple Mash they can save their work within. The subject leader can access this to look at pupil's work. If teachers wish to, they can also print of evidence directly from Purple Mash to stick into books. Teachers are also encouraged to save pupil's work in the 'shared area' on the school system.

- Formative feedback is given to pupils about their own progress in computing through discussion between teacher and children.
- Children are encouraged to save their work onto the network and Purple Mash independently. Each class teacher can then access children's files to view their work.
- Pupils' achievements will be reported to parents in the summer term as part of the annual report.

Staff Development

3.12 At Layfield it is vital that all teachers are confident and competent in the use of computing:

- We want to provide professional growth by identifying and taking into account individual staff's needs and aspirations and the school's needs.
- Staff are encouraged to improve their own performance and that of others and are encouraged to learn and develop effectively.
- We are committed to ensuring equality of opportunity and inclusion in the development of all staff.
- Staff understand the impact that the development of people has on the performance of our school, on our teams and on individuals.
- The Senior Management Team is supportive of the development of all our staff.

Resources:

Hardware

4.1 All classes have one computer in their room which is connected to the school network and gives access to school resources, software and the Internet. Each class has an Interactive Whiteboard which has replaced the traditional whiteboard.

4.2 Our computing equipment contains 17 desktop computers and 23 laptops, 1 desktop apple mac and 6 macbooks. We have a projector, 8 digital cameras, video recorders, video camera, a DVD player and a plethora of other electrical appliances. There are also 15 ipads to support learning. All hardware appliances are audited each year and updated as hardware is changed or added. At Layfield we have a commitment to renew equipment regularly to reflect current and developing technologies.

4.3 Each teaching member of staff is provided with a school laptop which is registered in line with DfES regulations. Every staff laptop is encrypted for added security. Each teacher is required to fill in a laptop protocol form; this constitutes an agreement that they will be used in accordance with school policy.

Their use is monitored in the same way as the school computers are.

- Everyone must log on to the school network using their secure log on.
- All machines should be locked when the user is away from the machine.
- Only machines accessing through the cache pilot are allowed (no personal machines or handheld devices).

4.4 A full hardware audit is available on the shared area.

4.5 For insurance purposes, all computing equipment needs to be locked away at the end of the day. Teachers are each responsible for the computers in their room and share responsibility for the computing suite. Each teacher is asked to sign an Acceptable Internet Use Statement. Staff have training in Data Protection and Information Security. In the suite the laptops must always be placed in the correct slot so they can be easily accounted for and the trolley must be locked at the end of each session. The number code for padlock on laptop cupboard is changed regularly for added security.

Cameras and Video Cameras

4.6 Cameras are available in school and are shared between staff. Staff also have use of tablets which can be used to record images and video. Once staff have finished with images they are actively encouraged to remove images and copy them onto the school system.

4.7 School cameras and tablets are for school use only and should not be taken home. Staff members should not use personal equipment (cameras or mobile phones) to take photographs or other images of pupils.

4.8 All images taken using the school cameras or tablets should be uploaded onto the network and if required for records or classwork, printed out at school. Staff should not keep images of pupils on their memory sticks.

4.9 Consent for using images of pupils for use on the school's newsletters, website or for media purposes is obtained from parents upon enrolment to school.

Mobile Phones

4.10 The use of mobile phones and other digital devices by pupils in school is not permitted. Phones brought to school by pupils are done so at the owner's risk and are the responsibility of the pupil.

4.11 The use of mobile phones by staff is only permitted when pupils are not present or in the staff room.

Interactive Whiteboards

4.12 Each class within school has an Interactive Whiteboard and teachers are monitored to ensure they are being used to their full potential. Where appropriate, lessons make use of digital resources and are interactive as to ensure that the children are fully stimulated and enthused.

Software

4.13 A wide-range of software is available on the network to suit the varied curriculum that we cover. There is a suitable selection of software available to facilitate the teaching of computing and create cross-curricular links.

4.14 Software is stored in the computing cupboard along with the manuals to enable access to all. The central resources are the responsibility of the Computing Subject Leader. An audit of all software and licences is kept. This audit is updated regularly.

4.15 Computing resources are valuable and sensitive to the environment in which they are stored. Care should be taken when moving them around school.

Health and Safety Issues in computing.

4.16 As in all subjects, health and safety aspects need to be considered, planned for and risks removed where possible. In computing all users need to be made aware that to reduce risks of injury we need to:

- Use of correct seating whenever computing is used.
- Ensure that there are adequate ventilation / air changes.
- Monitors should be checked for height and angle of view and moved if necessary (placing them back before leaving the equipment).
- Ensure cabling is made secure and kept out of sight wherever possible.

The Internet

The Importance of the Internet in School:

5.1 The purpose of Internet access in school is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems.

5.2 The statutory curriculum expects pupils to learn how to locate, retrieve and exchange information using computing. In order to deliver the curriculum, teachers need to plan for and make use of communications technology.

5.3 Access to life-long learning and employment increasingly requires computer and communications use and pupils need to develop life skills in their use.

5.4 Home and social Internet use is expanding and it is now an important part of learning and communication during leisure time. It brings pupils into contact with a wider range of information, the scope and nature of which may or may not be appropriate for the pupil. Whilst we cannot be responsible for internet use outside of school, at Layfield Primary we feel it is important to work with children and parents to ensure that all are informed in how to stay safe and use the internet responsibly.

PREVENT and Radicalisation

5.4 (a) Radicalisation is defined as the act or process of making a person more radical or favouring of extreme or fundamental changes in political, economic or social conditions, institutions or habits of the mind.

Extremism is defined as the holding of extreme political or religious views.

The Governing Bodies of Layfield Primary School has a zero-tolerance approach to extremist behaviour for all school community members. We rely on our strong values and ethos to steer our work and ensure the pastoral care of our children protects them from exposure to negative influences. Layfield School is fully committed to safeguarding and promoting the welfare of all its children. As a collaboration, we recognise that safeguarding against radicalisation is no different from safeguarding against any other vulnerability and therefore we teach children how to use the internet safely and what to do if they see anything they find unsettling. All staff and pupils are expected to uphold and promote the fundamental principles of British values, including democracy, the rule of law, individual liberty and mutual respect, and tolerance of those with different faiths and beliefs both online and inside of school. We teach regular E-Safety sessions within school to promote safe internet use and this complements the key “British Values” of tolerance, respect, understanding, compassion and harmonious living.

How are the risks assessed?

5.5 At Layfield Primary school we understand that in common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. It is difficult to completely remove the risk that pupils might access unsuitable materials via the school system but we have a number of systems in place to limit these risks.

- The use of computer systems without permission or for purposes not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990;
- Methods to identify, assess and minimise risks are constantly reviewed by the school, in partnership with the Local Authority.
- Staff, parents, governors and advisers work to establish agreement that every reasonable measure is being taken;
- Children are regularly given e-safety training at least at the start of every term so that they are aware of how to keep themselves safe, minimise exposure to unsuitable material and how to report anything that they feel is unsuitable.

How does school ensure Internet access is safe?

5.6 Our internet service is provided by Stockton Borough Council and at Layfield Primary school we are therefore protected by the Stockton LA content filtering system which is maintained by One IT. There are mechanisms and procedures in place to delete unsuitable websites through global and local blocking strategies and filtering.

- Offensive and illegal material is filtered at a national level.
- Inappropriate sites are then filtered at local level. Teachers can bring sites of educational value through the cache pilot by filling in the white list request form, stating their reasons for unblocking the site. The relevant site will, if authorised be passed to One IT for unblocking.

5.7 In school, children are taught how to use the internet to search for information. They are taught the skills necessary to do this and also about its appropriateness and safety implications.

- Pupils and teachers are informed that Internet use is supervised and monitored;
- The school works in partnership with parents, the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are

reviewed and improved;

- If staff or pupils discover unsuitable sites, the URL (address) and content are reported to the Internet Service Provider via the Computing Subject leader;
- Any material that the school suspects is illegal will be referred to the Internet Watch Foundation;
- Pupils are made aware that the writer of an e-mail or the author of a Web page might not be the person claimed;
- Pupils are encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.
- Annually the school celebrate 'Safer Internet Day'.

5.8 However, computing teaching should be widened to incorporate Internet content issues:

- The value and credibility of Web materials in relationship to other media. The tendency to use the Web when better information may be obtained from books may need to be challenged.
- Pupils are taught ways to validate information before accepting that it is necessarily accurate;
- Pupils are taught to acknowledge the source of information, when using Internet material for their own use;
- Pupils are taught at an age appropriate level about the dangers that the internet exposes and are taught how to keep themselves safe.

How is security of school computing systems maintained?

5.9 The Internet is a connection to the outside world that could compromise system performance or threaten security.

- Security strategies are discussed and reviewed with the LA on a regular basis;
- The security of the whole system is reviewed with regard to threats to security from Internet access;
- Virus protection is installed and updated regularly;
- Staff and Pupils scan any data storage devices before connecting them to the school network.

How is Internet access authorised?

5.10 All staff and pupils sign an agreement of responsible internet use when they join Layfield. They are then reminded of this each year with the invitation to discuss any concerns that may arise from it.

5.11 Everyone has a personal log on for which they are responsible. Log on's are monitored by staff and the Local Authority. Additional Log on's are requested through the Computing Subject Leader and are created in school.

- Internet access is a necessary part of the curriculum. It is an entitlement for pupils based on responsible use;
- Parents are informed that pupils are provided with supervised Internet access
- Parents, pupils and staff are asked to sign a responsible use agreement

form.

- Children are now asked to review this responsible use form each year & sign it again as part of their class.

Responsible use agreements:

5.12 All staff at Layfield Must agree to the following before using any piece of computing equipment:

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

5.14 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 computing system must not be compromised whether owned by the school, by Stockton Borough Council or any other organisation or individual.
- 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.
- Users should not deliberately seek out inappropriate or offensive materials on the internet (LA's recommended guidelines will be followed if needed).
- 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.
- Anything transferred from the school network with sensitive data in it i.e. children's names and dates of birth must be password protected. This includes e-mails and the learning platform.
- Only encrypted portable memory devices are to be used in school. Any sensitive data should be protected by 2 levels of security e.g. encrypted vault and encrypted file with separate passwords. Sensitive data i.e. anything with a child's name on it, should never be attached to the school learning platform.

- Only school equipment is to be used on the school network and internet system. Personal laptops and other mobile devices including 3G/4G mobile phones are not to be connected to the school system.

- All Internet use should be appropriate to staff professional activity or to student's education. However please note that:

- The school's computing system may be used to follow legitimate private interests, providing school use is not compromised.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Closed discussion groups can be useful but the use of public chat rooms and social networking is not allowed.

5.15 Staff should sign a copy of the Acceptable Internet Use Statement and return it to the Headteacher – See Appendix 1

5.16 All Children at Layfield Must agree to the following before using any piece of computing equipment:

5.17
Key Stage 1:

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

Key Stage 2:

Think then Click

e-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don’t know.
- We do not open e-mails/attachments/SMS sent by anyone we don’t know.
- We do not use Internet chat rooms or social networking

How are complaints regarding Internet use handled?

5.17 Prompt action is required if a complaint is made. The facts of the case need to be established, for instance whether the issue has arisen through Internet use inside or outside school. Transgressions of the rules could include minor as well as the potentially serious and a range of sanctions will be required, linked to the school's behaviour policy.

- Responsibility for handling incidents are given to senior members of staff;
- Parents and pupils will need to work in partnership with staff to resolve issues;
- As with drugs issues, there may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies;
- A pupil may have e-mail, Internet or computer access denied for a period of time depending on the nature of the incident;

How is parents' support enlisted?

5.18 Internet use in pupils' homes is increasing rapidly. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. The school may be able to help parents plan appropriate, supervised use of the Internet at home.

- A careful balance between informing and alarming parents is maintained;
- As and when needed, demonstrations and practical IT sessions for parents are organised to encourage a partnership approach;
- Joint home / school guidelines on issues such as safe Internet use will be established and literature from trusted child safety partners will be passed to parents.

Communication and Collaboration

E-mail

5.19 E-mail is now an essential means of communication within education and in the wider world.

- Pupils need to use e-mail as part of the National Curriculum 2014 Curriculum.
- Pupils in KS1 and KS2 are exposed to the principal on emails through the Purple Mash Curriculum. Where through their time at Layfield they are exposed to emailing several times in units of work they complete.
- All children are aware that e-mails sent through the school system are filtered.
- Children are made aware that in-coming e-mail is regarded as public. Received e-mail may be examined and could, for example, be pinned to a notice board for collection by pupils;
- Pupils in KS2 are allowed to access personal e-mail from the school system; and are taught to use it responsibly.

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education within school and how it outweighs their risks / disadvantages:

	Staff & other adults				Students/Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	√							√
Use of mobile phones in lessons				√				√
Use of mobile phones in social time	√							√
Taking photos on mobile phones / cameras				√				√
Use of other mobile devices eg tablets, gaming devices		√						√
Use of personal email addresses in school, or on school network		√						√
Use of school email for personal emails				√				√
Use of messaging apps				√				√
Use of social media				√				√
Use of blogs				√				√

When using communication technologies the school considers the following as good practice:

- **The official *school* email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.** *Staff and students / pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).*
- **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.**
- **Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.** *These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.*
- *Whole class / group email addresses may be used at KS1, while students / pupils at KS2 and above will be provided with individual school email addresses for educational use*

Profiles

5.20 Online profiles need to be discussed with children as part of their e-safety training. Children are made aware of the dangers in releasing personal information and are taught to assess risk. Children are made aware that once something is posted on the internet it is very difficult to remove and they are taught to keep their information safe. Children may create online profiles and avatars in secure places e.g. school blogs.

Publishing

5.21 At Layfield we recognise the exciting opportunities that publishing online presents. By publishing work online, children are given a fantastic opportunity to gain a world-wide audience for their work. We want to encourage this but to also encourage responsible use.

- Copyright is always respected.
- Authors work own work is always recognised.
- Approval is always sort from an adult before uploading to the web.
- Public chat rooms are not allowed in school, however, children may use managed notice boards and discussion groups.
- Children's images should only be shared after seeking permission from an adult and should be checked against parental permissions list.

Video Conferencing

5.22 This is becoming a widely recognised and used educational tool. It allows more personal communication and collaboration but must always be used responsibly and safety.

- Conferencing and webcams may only be used when a member of the teaching staff is present and has given their permission.
- A safe portal must be used.
- When not in use the webcam or recording equipment must have lens cap closed or be disconnected.
- Only children with permission to share their image should be included in a webcam broadcast.

School Website

5.23 At Layfield Primary School we have a fantastic website that inspires pupils to publish work to a high standard, for a very wide audience. Our web site celebrates pupils' work, promotes the school, informs parents of up and coming events, enables them to read school policies and can be used to publish resources for projects or homework. It is also used to communicate with parents current and prospective.

5.24 As the school's website can be accessed by anyone on the Internet, the security of staff and pupils are considered carefully.

- Home information or individual e-mail identities are not published;
- Only pupils who have permission to use their images are to have photographs published to the website.
- Full names will not be used anywhere on the Web site
- Children's names will not be placed next to visual media
- All publishing rules apply (copyright, authors recognition, teacher's permission needed before publishing).

Layfield Primary School

LAPTOP/DIGITAL DEVICE PROTOCOL FOR TEACHERS AND SCHOOL SUPPORT STAFF AND BRING YOUR OWN DEVICE (BYOD) PROTOCOL

This protocol is designed to act as a guide and simple framework upon which the use of laptops/digital devices by teachers or school support staff should be based. The intended spirit of the list is to act as a reminder on use and security. The opportunities offered via mobile technologies are vast as more and more online services become available for teaching and learning. This has led to schools allowing staff to bring in their own device in order to provide a greater choice and usability. However it is important that a number of e-safety considerations for BYOD have been explored. BYOD should not bring in e-safety concerns of issue into what should be a secure environment. Considerations may include secure access, filtering, data protection, storage and the transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. The above is not and exhaustive list. Below are guidelines for safe use of all devices within the school setting, however all usage must comply with the Acceptable Use Policy and school Computing Policy.

- The ownership of the laptops rests with the school. If the laptop/digital device does not belong to the school and is intended for use within school, the use of this item must be in line with the school's acceptable use policy.

- Teachers / support staff have full use of the laptops/digital devices to develop planning, curriculum subject and computing experience.

- Teachers / support staff are free to install software appropriate to their professional needs on the laptops/digital devices providing all licences are kept securely and they are in line with the acceptable use policy and school computing policy.

- No restrictions or barriers are placed on internet access; staff are free to choose their own ISP and are responsible for any charges incurred. All equipment, whether owned by the school or the individual should not be used to access inappropriate information such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act or inappropriate or may cause harm or distress to others.

- Teachers / support 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 for teaching and non-teaching staff should they do so.

- Anti-virus software is provided with each school laptop and members of staff have the responsibility of keeping the software up-to-date and for scanning materials downloaded from the Internet. Devices from outside of school owned by a visitor for use within school should be protected by anti-virus software to ensure no virus' can be transferred to the school systems.

- Teachers / support staff should always password protect important or sensitive information, and ensure that back-up copies of such information are taken and held securely. Information should only be taken by individuals using their own laptops/digital devices with accordance to the Acceptable Use Policy.

- There are a number of legal requirements relating to the use of information and software (eg Data Protection Act, Copyright Act). Teachers / support staff are responsible for understanding and complying with their legal requirements. Advice and guidance is available from the Stockton Schools' LA.

- Teachers / support staff should be aware that laptop computers/ digital devices have a high re-sale value and that they should never be left in cars or in a place where an opportunist could take it. With most insurance companies laptops are covered in cars as long as they are not left unattended.

- Teachers / support staff should make sure that they are aware of the arrangements that have been made by the school for insurance cover on laptop computers and to follow any guidelines / procedures established by the school to safeguard this cover. If an individual is bringing in their own digital device/laptop into school, it is their responsibility to ensure that their device is covered by an insurance company/provider.

- Be aware of the school's policy on the use of laptops and digital devices on the school network.

Staff should sign a copy of this Laptop Protocol and return it to the Headteacher.

Full name ……………………………… post ………………………………

Signed ……………………………… date ………………………………

Approved ……………………………… date ………………………………

Appendix 1

	Name of School	Layfield Primary School
	AUP review Date	February 2018
	Date of next Review	February 2019
	Who reviewed this AUP?	School Improvement Meeting of Governors

Staff (and Volunteer) Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school / academy ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to computing to enhance their work, to enhance learning opportunities for *pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of Computing for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of computing materials. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the *school w*ill monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) out of school. School equipment should not be used to access inappropriate information such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act or inappropriate or may cause harm or distress to others.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using *school* ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school as long as content is not harmful, offensive or degrading to any pupil/member of staff/parent of the school etc.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (schools should amend this section to take account of their policy on communications with students / pupils and parents / carers. Staff should be made aware of the risks attached to using their personal email addresses / mobile phones / social networking sites for such communications)
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the *school*

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will also follow any additional rules set by the *school* about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school / academy ICT systems unless I ask the designated Computing Lead.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

When using Social Media:

- Staff must not access social networking sites for personal use via school information systems or using school equipment;
- Staff must not accept pupils as friends – personal communication could be considered inappropriate and unprofessional and makes staff vulnerable to allegations;
- Staff are advised not to be friends with recent pupils. The potential for staff to be compromised in terms of wall content and open to accusations makes the risk not worth taking;
- Staff should not place inappropriate photographs on any social network space;

- Staff should not post indecent remarks;
- If a member of staff receives messages on his/her social networking profile that they think could be from a pupil they must report it to their Line Manager/Headteacher and contact the internet service or social networking provider so that they can investigate and take the appropriate action;
- Staff are advised not to write about their work but where a member of staff chooses to do so, he/she should make it clear that the views expressed are his/hers only and do not reflect the views of the school/Local Authority. However, all other guidelines in this policy must be adhered to when making any reference to the workplace;
- Staff must not disclose any information that is confidential to the school or disclose personal data or information about any individual/colleague/pupil, which could be in breach of the Data Protection Act;
- Staff must not disclose any information about the school/Local Authority that is not yet in the public arena;
- In no circumstances should staff post photographs of pupils;
- Staff should not make defamatory remarks about the school/colleagues/pupils or the Local Authority or post anything that could potentially bring the school/Local Authority into disrepute;
- Staff should not disclose confidential information relating to his/her employment at the school;
- Care should be taken to avoid using language which could be deemed as offensive to others;
- Staff should make sure they understand the school's social media policy;
- Staff should not leave computers or other devices logged-in when unattended;
- Staff should preferably use a pin or passcode on mobile phones or similar devices in case they are lost or stolen;
- Staff should be familiar with the privacy and security settings of social media apps used and keep them up to date; [the UK Safer Internet Centre website's reputation page has more information: www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/professional-reputation];
- Staff should be aware that their reputations can be harmed by what others share about them online - for example, being tagged in inappropriate posts, videos or photographs;
- Staff should consider their own conduct online - some behaviour could breach the employment behaviour policy or code of conduct;
- Staff should discuss issues with colleagues, close family and friends to ensure they have appropriate privacy and security settings;
- Staff should not give out personal contact details. If pupils need to contact a member of staff they should be given the school's contact details;
- Staff should ask for a school mobile phone to be issued to staff on school trips rather than using a personal phone; and
- Staff should keep their school email address for school business and their personal email address for private communications.

I understand that I am responsible for my actions in and out of the *school*:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, referral to Governors and in the event of illegal activities the involvement of the police.

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

Staff / Volunteer Name	
Signed	
Date	