Computing Policy

February 2020

Review Date: February 2022

Content:

Context

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.

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 2020 by Mr L Barker

To be revised again: February, 2022

Intent Statement

At Layfield Primary School, we recognise the importance of Computing and its importance in an ever-changing technological world. We want all pupils to develop a love for computing and strive to reach their full potential with the vast array of technology available to them. We strive to develop technological curiosity and provided pupils with fun, inspiring computing links within our curriculum. Memorable experiences through visitors and visitors aim to provide pupils with opportunities to learn important life skills such as E-Safety. Throughout the computing curriculum, pupils are challenged to develop as an individual, to overcome problems, discover new skills and strive to be empowered by technology.

Our Vision for Computing:

At Layfield we believe that:

- 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.

We can achieve this vision by:

- Providing an exciting, rich, relevant and challenging Computing curriculum for all pupils.
- 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 the confidence to experiment with new software and apply their developing skills in new contexts.

3

- 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.

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, respectful and competent users of data, information and communication technology.

Principles for the use of computing

Computing education is important because:

- It equips pupils to use computational thinking and creativity to understand and change the world.
- It equips pupils with skills, strategies and knowledge that will enable them to reap the benefits of the online world, whilst being able to minimise risk to themselves or others.
- 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.

<u>Teaching and Learning</u>

Safeguarding

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.

National Curriculum

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.

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

As a school, we have chosen the Purple Mash Computing Scheme of Work. The scheme of work supports our teachers in delivering fun and engaging lessons which help to raise standards and allow all pupils to achieve to their full potential. We are confident that the scheme of work more than adequately meets the national vision for Computing. Furthermore, it gives excellent supporting material for less confident teachers.

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

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.

Key Stage Outcomes

Key Stage 1 outcomes:
- Understand what algorithms are, how they are implemented as programs on digital devices, and that programs execute by following a sequence of instructions.
- Write and test simple programs.
- Organise, store, manipulate and retrieve data in a range of digital formats.
- Communicate safely and respectfully online, keeping personal information private, and recognise common uses of information technology beyond school.

Key Stage 2 outcomes:
- Design and write programs that accomplish specific goals, including controlling or simulating physical systems; solve problems by decomposing them into smaller parts.
- Describe how Internet search engines find and store data; use search engines effectively; be discerning in evaluating digital content; respect individuals and intellectual property; use technology responsibly, securely and safely.
- Use sequence, selection and repetition in programs; work with variables and various forms of input and output; generate appropriate inputs and predicted outputs to test programs.

5

- Select, use and combine a variety of software (including internet services) on a range of digital devices to accomplish given goals, including collecting, analysing, evaluating and presenting data and information.
- Use logical reasoning to explain how a simple algorithm works and to detect and correct errors in algorithms and programs.
- Understand computer networks including the internet; how they can provide multiple services, such as the worldwide web; and the opportunities they offer for communication and collaboration.

Cross-curricular Links

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

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

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

At Layfield Primary School, we aim to enable all children to achieve to their full potential. This includes children of all abilities, social and cultural backgrounds, those with disabilities, EAL speakers and SEN statement and non-statemented. We place particular emphasis on the flexibility technology brings to allowing pupils to access learning opportunities, particularly pupils with SEN and disabilities. With this in mind, we will ensure additional access to technology is provided throughout the school day and in some cases beyond the school day.

Assessment, Monitoring and Evaluation

Staff are provided with the curriculum framework from the Purple Mash Whole school curriculum, which ensures that children across all key stages are provided with opportunities to achieve end of key stage expectations. This framework includes a clear progression of skills which ensures that children are making progress. Staff can therefore use the progression documents to ensure that any gaps in pupils learning are targeted and filled.

Monitoring standards of teaching and learning within Computing is the primary responsibility of the Computing Leader. Monitoring termly enables the subject leader to gain an overview of Computing and ICT teaching and learning throughout the school. This will assist the school in the self-evaluation process identifying areas of strength as well as those for development.

In monitoring the quality of Computing and ICT teaching and learning, the subject leader will:

- Observe teaching and learning in the classroom.
- Hold discussions with teachers and children.
- Analyse children's work
- Examine plans to ensure full coverage of the Computing and cross-curricular ICT

Staff Development

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

- Scheduled pupil voice sessions and learning walks steer changes and inform training needs.
- 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.
- Training for staff and governors is relevant to their needs and ultimately positively impacts on the pupils.
- 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

At Layfield, a range of resources are available, which successfully supports delivering the Computing curriculum and enables all learners to reach their full potential.

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.

Our computing equipment contains 17 desktop computers and 23 laptops. There are also 15 iPads to support learning alongside staff ipads.

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. Resources are suitably maintained and replenished when needed, which is overseen by the Computing Leader and ONEIT.

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.

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).

A full hardware audit is due to be added to the shared area.

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

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.

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.

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.

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

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. Pupils in Year 5 and 6, who do bring phones into school, have the device locked in a filing cupboard for the day and handed back to them at the end of the school day.

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

Interactive Whiteboards

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

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.

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.

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.

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:

9

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.

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.

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

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 that 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?

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.

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'.

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?

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?

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.

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:

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

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.

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.

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

All Children at Layfield must agree to use all equipment with respect and safely. Following our 3 school rules of Ready, Respect and Safe at all times.

How are complaints regarding Internet use handled?

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?

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

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:

Communication Technologies	Staff & other adults				Students/Pupils			
	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 (e.g. 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

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
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.
- Author's 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

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

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.

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).

17

1590 Trust
Staff Acceptable Use Agreement & Code of Conduct

Full Name ……………………………………………….. (print)

School/Department……………………………………………………………………………

Signature ………………………………………………………………Date ……………

ICT (including data) and the related technologies such as email online services (including data sharing), the internet and mobile devices are an expected part of our daily working life in school. This policy 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 follow it at all times. Any concerns or clarification should be discussed with the school headteacher or Director of IT Services.

1. I acknowledge that ICT includes a wide range of systems, including (but not exclusively) mobile phones, digital cameras; email, online cloud services and social networking. ICT use may also include personal devices when used for school business.

2. I will only use the school's data sharing/ email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable and appropriate' by the Headteacher or the Governing Body.

3. I will comply with the ICT system security protocols and not disclose, publish or share any data or passwords provided to me by the school or other related authorities. I will not use personal accounts for work based activities in any way.

4. I will ensure that all electronic communications with students and staff are compatible with my professional role.

5. I will not disclose my own personal details, such as mobile phone number and personal email address, to students. This also includes sharing school based data in systems not endorsed by the trust.

6. Staff must not for any reason become digitally associated (e.g. 'friends / buddies') of students either internally or externally on any form of social networking site.

7. I will only use approved, secure email system(s) for any school business.

8. I will ensure that personal data (such as data held on MIS software or other official systems) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data, concerning staff and students, can only be taken out of school or accessed remotely, when authorised by the Headteacher or the Governing Body. Personal or sensitive data taken off site must be encrypted. Sensitive data must not be shared or sent to external parties, without explicit permission from the Headteacher.

9. I will not install any hardware or software on school the site or provided equipment without permission.

10. I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others; nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place which specifically prevent access to such content.

11. By using IT facilities or by connecting equipment (own/school provided) to school systems you agree to the trust using filtering and monitoring software to ensure child safety and learning is focused upon.

12. If using school owned devices, I understand that the above may also be enabled if the device is taken off site.

13. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory, or bring the organisation into disrepute.

14. Multimedia (including images/video) of students 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 the Headteacher.

15. 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 my Line Manager or the Headteacher.

16. I will respect copyright and intellectual property rights and I will adhere to these and data protection laws.

17. I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

18. I will support and promote the school's E-safety Policy and help students to be safe and responsible in their use of ICT and related technologies.

19. I understand this forms part of the terms and conditions set out in my contract of employment.

Use of Online & Cloud Services

20. I will only use the official school provided systems for sharing resources and data. I agree to not share such data outside of the closed systems provided.

21. I will ensure that I will implement robust security, following school guidance in ensuring the protection of data online.

22. I will not share or communicate privately with students using school provided or any other online communication method. I agree to use only the systems provided.

23. I understand the need to report any suspected child protection or data breech concerns directly to the headteacher.

24. I understand that all use of school systems will be logged, and I will be subject to regular child protection checks.

25. I understand that all files / data produced for work purposes, remains the intellectual property of the trust.

26. The trust remains the right to terminate access to digital services on the grounds of child protection or part of data preservation protocols.