Allerton Grange Staff

School Policy for working in Educational Settings on the Use of Digital Technologies and Social Media

(Includes Allerton Grange Acceptable User Declaration)

Originator: Allerton Grange School / LCC CA 03/12/19

Key Links: NWa / ICS

CONTENTS

Section 1 - Overview

ICT and the internet are essential tools for teaching and learning and communication that are used in Allerton Grange School to deliver the curriculum, and to support and challenge the varied learning needs of its students. ICT is used to share information and ideas with all sections of the school community.

At Allerton Grange School, the use of the internet and ICT is seen as a responsibility and it is important that students and staff use it appropriately and practise good online safety. It is also important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

Online safety covers the use of the internet as well as mobile phones, electronic communications technologies and the use of social media and social networks. We know that some adults will use these technologies to harm students. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. Staff have a duty of care to protect children from risk of harm, as well as a duty to ensure their own conduct does not bring into question their suitability to work with children.

This guidance takes into account the principles of the Safer Working Practice Guidance (National Safer Recruitment Consortium) as well as guidance from the Department for Education (Safeguarding Children in a Digital World), CEOP (Child Exploitation and Online Protection) and Communication Act 2003 (Section 127 Improper Use of Public Electronic Communications Network). http://www.legislation.gov.uk/ukpga/2003/21/section/127

This guidance applies to all staff, employed either directly or indirectly by Allerton Grange School, as well as volunteers and staff not employed directly by the school, but based at the school. All staff are expected to adhere to this code of practice to ensure the safety of the students, young people and adults at risk, who they may come into contact with through their professional role. Any member of staff in breach of these guidelines may be subject to disciplinary action in accordance with the school's Disciplinary Policy and Procedure.

1.1 Definition of Students

For the purpose of this document, 'students' refer to children, young people and adults at risk in educational settings whom a professional may come into contact with, as a direct result of their role.

1.2 Adults at Risk: means adults who need community care services because of mental or other disability, age or illness and who are, or may be, unable to take care of themselves against harm or exploitation. The term replaces 'vulnerable adults'.

Section 2 - Responsibilities

Governors and headteachers are responsible for ensuring this guidance is shared with, and adhered to, by all staff.

Staff are responsible for their own actions and must act, and be seen to act, in the best interests of students at all times. Staff must ensure they understand and adhere to this guidance as well as

Allerton Grange School's expectations and Internet Acceptable Use Policy (included within this document). Staff are also responsible for acting promptly to prevent and safeguard students from potential abuse online and for reporting any concerns in accordance with the Leeds Children's Services Safeguarding & Child Protection Policy for Schools and Colleges.

Staff are solely responsible for any content and applications on their own personal social media networks and electronic devices, to ensure that they do not breach the school's safer working practice guidance, or undermine public confidence in the school or the education profession. This includes security and privacy settings when using social media, via their chosen equipment. Failing to ensure adequate and appropriate settings are in place, may lead to disciplinary action should the content be in breach of school expectations, professional conduct, and/or bring the school into disrepute.

Staff are also responsible for ensuring their own use of ICT and social media is professional and appropriate at all times. Staff must be aware that their conduct online, both inside and outside of school, must not breach the school's code of conduct or professional expectations. Any behaviour that is deemed to breach such expectations may be subject to disciplinary action.

Section 3 - Social Contact with Students

Staff must not establish, or seek to establish, social contact with students for the purpose of securing a friendship or to pursue or strengthen a relationship. Even if a student themselves seeks to establish social contact. If this occurs coincidentally, the member of staff should exercise their professional judgement in making a response and be aware that such social contact could be misconstrued. Staff should alert the headteacher, immediately, of any such contact.

All contact with students should be through appropriate channels at all times and should be within clear and explicit professional boundaries. This means staff should only contact students regarding school matters when in school, using school equipment and with appropriate permission from senior leadership.

Staff must not, nor be required to, give their personal details such as home or mobile number; social media identities; or personal email addresses to students. Any member of staff found to be in contact with students through any of the above means, or any other unapproved method, without prior consent from the headteacher/senior leader, may be subject to disciplinary action.

Internal email and approved contact systems should only be used in accordance with the appropriate ICT policy and/or Acceptable Use policy.

Section 4 - Social Media

In order to make best use of the many educational and social benefits of new and emerging technologies, students need opportunities to use and explore the digital world. Online risks are posed more by behaviours and values than the technology itself.

Staff should ensure that they establish safe and responsible online behaviours, working to local and national guidelines and acceptable use policies, which detail how new and emerging technologies may be used.

Communication with children both in the 'real' world, and through web-based and telecommunication interactions, should take place within explicit professional boundaries. This includes the use of computers; tablets; phones; texts; e-mails; instant messages; social media such as Facebook and Twitter; chat-rooms; forums; blogs; websites; gaming sites; digital cameras; videos; web-cams; and other hand-held devices. (Given the ever-changing world of technology, it should be noted that these are only examples and is not exhaustive.)

Staff should not have contact with students using social media and, specifically, social networking sites without prior permission from the headteacher. Staff must not add students as 'friends' or respond to 'friend requests' from them. If a member of staff suspects that an existing 'friend' is a student, child or young person, they must take reasonable steps to check the identity of the individual and end the social media friendship.

It is recognised that personal access to social networking sites outside the work environment is at the discretion of the individual. However, members of staff should consider their use of social networks as they take on the responsibilities of a professional; taking particular care to secure personal information. They should ensure their use of such networking sites is respectable and appropriate at all times.

Secure and suitable 'strength' passwords should be devised and security settings should be applied when accessing your profile, and the information contained within it, so that it is limited to only those explicitly given access. Users should not sign up to non-work-related web-accounts using a work email address or password.

It is also advisable to log out of any sites on a personal computer or an application on a mobile device to ensure maximum security. Activities undertaken by others who can have access to your social media platforms, shall be deemed attributable to the user logged in at the time, unless there is a good and verifiable reason to suspect otherwise (e.g. hacking).

Understand and check your privacy settings on your social media profiles so you can choose to limit who has access to your data. You may also want to consider how much personal information you include on your profile.

Personal profiles on social networking sites and other internet posting forums should not identify your employer or place of work and careful consideration should be given to information, which is published on such sites. For example, information which is confidential, damaging to the school or undermines public confidence in the school's reputation.

All postings to social media websites should be considered in the public domain. Therefore, only post comments, videos and pictures, which you would be happy to share with any group of friends, strangers or colleagues. Do not post information, which could lead to the identification of someone connected to the school or your profession without their explicit consent. This includes posting images of people. Remember once you have published information you cannot guarantee it can be fully removed, and you cannot control how it is shared.

Material published by staff in a social context, which is considered to bring the school into disrepute, or considered harmful to, or harassment of a student, colleague or member of the school community, will be dealt with under the disciplinary procedure.

Subject to the constraints within this policy, it is understood that employees have the right to free expression of opinion in their lives outside school, including on matters of public policy.

Section 5 - Creating Images of Students through Video or Photography

Many work-based activities involve recording images and these may be undertaken as part of the curriculum, extra school activities, for publicity, or to celebrate achievement. However, written explicit consent must be gained from legal guardians as well as senior management prior to creating any images of students.

Using images of students for publicity purposes requires the age-appropriate consent of the individual concerned and their legal guardians. Images should not be displayed on websites, in publications or in a public place without such consent. The definition of a public place includes areas where visitors to the school or service provision have access. Consent to use images can be withdrawn at any time, without giving a reason and, in such cases, staff must make every effort to remove/destroy these images wherever they have been published.

Photographic or video images must be created using equipment provided by the work place. It is not acceptable to record images of students on personal equipment such as cameras, mobile phones or video camera. Images of students must not be created or stored for personal use.

Members of staff creating or storing images of students using personal equipment without prior consent will be subject to disciplinary action.

Members of staff must:

- be clear about the purpose of the activity and what will happen to the photographs when the lesson/activity is concluded;
- ensure that senior management is aware that photography/image equipment is being used and for what purpose;
- ensure that all images are available for scrutiny, in order to screen for acceptability; and be able to justify images of students in their possession;
- ensure that images are held only for as long as necessary for the 'purpose'. The recommendation for images of children and young people is that they should be held no more than 2 years;
- avoid making images in one-to-one situations.

Members of staff must not take, display or distribute images of students unless they have explicit written consent to do so. Failure to follow any part of this code of practice may result in disciplinary action being taken.

For further guidance on creating, displaying and storing images of students, please refer to the Safer Working Practice Guidance (National Safer Recruitment Consortium); as well as guidance from the Department for Education (Safeguarding Children in a Digital World); and CEOP (Child Exploitation and Online Protection).

Section 6 - Use of personal technology/equipment in school

The use of any personal equipment in schools should always be with the prior permission of senior management in order to comply with health and safety regulations, safer working practice guidance, data protection and school policies. Members of staff should take care to comply with acceptable use and ICT policies.

Personal equipment capable of recording and/or moving images or sounds, and those used for accessing the internet, such as mobile phones, cameras, video cameras and laptops, should not be used in work time without the prior permission of senior management.

Any member of staff found to be using such personal equipment without prior authorisation may be subject to disciplinary action in accordance with the School's Disciplinary Policy and Procedure.

Section 7 - Internet Use

Members of staff must follow and adhere to the policies on the use of IT equipment at all times and must not share logins or password information with other members of staff, students, children or young people, friends, family or members of the public.

As a general principle, internet access is provided to employees to support work-related activities. The following list is not intended to be exhaustive, but sets out broad areas of use that the school considers to be acceptable uses of the internet.

7.1 Acceptable Use

- To provide communication within the school via email or the school website
- To provide communication with other schools and organisations for educational purposes
- To distribute details regarding school meetings
- To provide electronic methods of communication
- Any other use that directly supports work-related functions.

7.2 Unacceptable Use

The following uses will be regarded as 'not acceptable' irrespective of the means of internet access:

- Using the computer to perpetrate any form of fraud, or software, film or music piracy
- Use for racial, sexual, homophobic or other harassment.
- To access pornographic, obscene or illegal material.
- To solicit personal information with the intent of using such information to cause emotional or physical harm.
- Entering into a commitment on behalf of the school (unless you have explicit permission to do this).
- Visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material.

- Downloading commercial software, or any copyrighted materials, belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence.
- Hacking into unauthorised areas.
- Publishing defamatory and/or knowingly false material about Allerton Grange School, your colleagues and/or our students on social networking sites, 'blogs' (online journals), 'wikis' or any other online publishing format.
- Revealing confidential information in a personal online posting, upload or transmission, including financial information and information relating to our students, staff and/or internal discussions.
- Use of personal email to communicate with, or about, any students of Allerton Grange.
- Introducing any form of malicious software into the corporate network.
- Disrupt the work of other users, for example, the propagation of computer viruses.

Section 8 - Confidentiality and Security

The storing, and processing, of personal information is governed by the General Data Protection Regulation and Data Protection Act. Employers are required to provide clear advice to staff about their responsibilities under this legislation so that, when considering sharing confidential information, the principles set out in the legislation apply.

Members of staff may have access to confidential information about students and families and the organisation in order to undertake their everyday responsibilities. In some circumstances, this may be highly sensitive or private information and should only be shared when legally permissible to do so, and in the interest of the child. Records should only be shared with those who have a legitimate professional need to see them.

Only authorised school-based devices and systems should be used to store and transfer confidential information. Developments in technology have improved the security of email. This has meant that Leeds City Council has been able to follow centrally issued guidance to protect personal and special category data sent by standard email. When email services are configured appropriately at BOTH ends of the route, email is just as good as Mail Express or any other secure data transfer mechanism, once controls are in place.

For further guidance in relation to sending personal information electronically, please refer to the guidance titled 'Exchanging data electronically'. Members of staff found to be compromising confidentiality by use of unauthorised systems and devices could be subject to disciplinary action.

For further guidance in relation to confidentiality, issues and safe storage of data please refer to the Safer Working Practice guidance document.

Section 9 - Cyber Bullying

All forms of bullying, including cyber bullying, are taken very seriously. Bullying is never tolerated. It is not acceptable for any member of staff to behave in a manner that is intimidating, threatening, or in any way discriminatory. Behaviour which constitutes bullying or harassment may be dealt with under the Grievance/Bullying and Harassment Policy and could result in disciplinary action.

However, this does not just extend to behaviour within the work place. In some instances, bullying or harassment that occurs outside the workplace, where there is a link to employment, could also fall under the responsibility of the employer and, therefore, result in disciplinary action being taken against the responsible individual.

Certain activities relating to cyber bullying could be considered a criminal offence under a range of different laws. Cyber bullying consists of threats, harassment, embarrassment, humiliation, defamation or impersonation and could take the form of general insults, prejudice based bullying or discrimination through a variety of media. Media used could include email, virtual learning environments, chat rooms, websites, social networking sites, mobile and fixed-point phones, digital cameras, games and virtual world sites.

If an allegation is received where a member of staff is responsible for comments made online, which could be deemed harmful, threatening, defamatory, abusive or harassing in any way towards another employee, the school will investigate this matter. Any allegation of bullying or harassment made by an employee against another member of staff where the accused uses the internet, mobile phone, text message or email, along with any other forms of abuse, may be dealt with through the Grievance/Bullying and Harassment Policy and could lead to disciplinary action.

Staff are required to take steps to protect themselves and their personal information by:

- keeping all passwords secret and protect access to their online accounts;
- not befriending students and young people on social networking services and sites;
- keeping personal phone numbers private;
- not using personal phones to contact parents, students and young people;
- keeping personal phones secure, i.e. through use of a pin code;
- not posting information about themselves that they wouldn’t want employers colleagues, students, young people or parents to see;
- not retaliating to any incident;
- keeping evidence of any incident;
- promptly reporting any incident using existing routes for reporting concerns.

School staff, as well as students, may become targets of cyberbullying. Staff should never retaliate by personally engaging with cyberbullying incidents. They should report incidents appropriately and seek support.

Staff should report all incidents to their designated line manager or member of the senior leadership team. The designated person will take responsibility for ensuring that the victim is supported; investigating and managing the incident; and contacting the police and local authority, if appropriate.

For various reasons, staff may find it difficult to report to their line manager in the first instance. They may want additional support or advice. They should know that they can seek advice and help from their union, professional association, education support partnership, or other organisation.

Further information and advice regarding cyberbullying can be found in the DfE guidance documents Preventing and Tacking Bullying and Cyberbullying: Advice for Head Teachers and School Staff. https://www.gov.uk/government/publications/preventing-and-tackling-bullying

Section 10

Policy Introduction to Students and Parents

Many students are very familiar with the culture of mobile and Internet use. However, as students' perceptions of the risks will vary, the online safety rules may need to be explained or discussed.

Allerton Grange will ensure:

- all users will be informed that network and Internet use will be monitored;
- students are trained and informed of safe and responsible internet use;
- safe and responsible use of the internet and technology is reinforced across the curriculum and subject areas;
- particular attention to online safety education will be given where students are considered to be vulnerable.

Allerton Grange is able to help parents plan appropriate, supervised use of the Internet at home, and educate them about the risks.

Parents will be:

- drawn to the school's online safety guidance in newsletters, school prospectus and on the school website;
- a partnership approach to online safety at home, and at school, with parents will be encouraged. This may include offering parents' evenings with demonstrations and suggestions for safe home internet use, or highlighting online safety at other attended events e.g. parent evenings.

Section 11

Allerton Grange Staff Acceptable Use Declaration

The school has provided computers for use by staff as an important tool for teaching, learning, and administration of the school. Use of school computers is governed at all times by the following policy.

Please ensure you understand your responsibilities under this policy, and direct any questions or concerns to Ian Thompson / Natalie Watson in the first instance.

All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. Deliberate abuse or misuse of the school's computer system may result in disciplinary action (including possible termination), and civil and/or criminal liability. Please note that use of the school's network is intended to be as permissive and flexible as possible under current UK legislation and DfE guidelines. This policy is not intended to arbitrarily limit the ways in which you can use the system, but to ensure compliance with the legal responsibilities of the school and staff, in order to safeguard the reputation of the school, and ensure the safety of all users. Please respect these guidelines, many of which are in place for your protection. Lastly, the school recognises that the distinction between computer-use at work, and at home, is increasingly blurred, with many of us now using our own computers for work. While the school neither wishes nor intends to dictate how you use your own computer, staff should consider that the spirit of this policy applies whenever you are undertaking an activity that stems from your employment with the school.

Computer Security and Data Protection

- You will be provided with a personal account for accessing the computer system, with your own username and password. This account will be tailored to the level of access you require, and is for your use only. As such, you must not disclose your password to anyone. If you do so, you will be required to change your password immediately. IT Admins may require your password to aid in resolving issues, they will keep your password securely and erase after use.
- Passwords need to meet a minimum security requirement.
  - 8 characters in length
  - Must contain at least 3 of the following: symbol, number, capital, lower case letter.
  - Passwords cannot be your name or previous password
- Access to email is permitted on school and personal owned phones and tablets. These devices are required to have an access code. Either alphanumeric or numeric at least 8 characters in length.
- You must not allow a student to have use of a staff account, under any circumstances, for any length of time, even if supervised.
- When leaving a computer unattended, you must ensure you have either logged out of your account, or locked the computer to prevent anyone using it in your absence.
- You must not let your staff laptop be used by any colleague (unless handed to IT support for fixing), family member or friend.
- Downloads may be restricted or blocked even from vendors you may recognise as safe. This is to protect the school network from virus attack.
- You must not store any sensitive or personal information about staff or students, (this includes names) on any portable storage system (such as a USB memory stick, portable hard disk, or personal computer).
- The school has the right to remove access to unencrypted or encrypted USB devices at any point.
- The school provides cloud storage for staff and students. Our approved Cloud storage provider is Microsoft OneDrive.
- You must not use Dropbox and iCloud as they do not meet Ofsted or GDPR requirements.
- You must not transmit any sensitive or personal information about staff or students, via email, outside the school system without the data being encrypted by a method approved by the school.
- Before sending any sensitive or personal information about staff or students. You need to establish why this information is required and if they fully comply with GDPR laws. If you are unsure, please speak to IT Manager, Ian Thompson and/or Natalie Watson, HR Director.
- When publishing or transmitting non-sensitive, sensitive or personal data material i.e. a photo outside of the school, you should take steps to protect the identity of any student whose parents have requested this.
- If you use a personal computer at home for work purposes, you must ensure that any school-related sensitive or personal information is secured, to prohibit access by any non-member of staff, and encrypted to protect against data loss and theft.
- You should make your own backup of data kept on any storage system other than the network storage drives or your ‘My Documents’ folder. This includes USB memory sticks

(even those owned or issued by the school), school laptops or a personal computer and anything saved on the school desktop.

- You should ensure that items of portable computer equipment (such as laptops, digital cameras or portable projectors) are securely stored in a locked room or cupboard when left unattended.
- Equipment taken offsite is not routinely insured by the school. If you take any school computer equipment offsite, you should ensure that adequate insurance cover has been arranged to cover against loss, damage or theft. Please discuss this with the Finance Director.

Personal Use

The school recognises that occasional personal use of the school's computers is beneficial, both to the development of your ICT skills and for maintaining a positive work life balance. Such use is permitted, with the following conditions:

- It complies with all other conditions of this document as they apply to non-personal use, and all other school policies regarding staff conduct.
- It does not interfere, in any way, with your other duties or those of any other member of staff.
- It does not have any undue effect on the performance of the computer system.
- It Is not for any commercial purpose or gain unless explicitly authorised by the school.
- It is at your own risk when entering any personal or sensitive data into websites.
- Personal use is permitted at the discretion of the school and can be limited or revoked at any time.
- Access to social network sites or multimedia platforms is restricted unless you require this for your role within school. Regardless if you use a school or personal owned device.

Use of your own equipment

- Any mains-operated personal computer or electrical equipment brought on site, for any use, is subject to a Portable Appliance Test (PAT) by site maintenance staff, and must not be used until approved. This test must be performed at regular intervals as required by school's normal rules on electrical safety testing.
- You must not connect your personal device to a school computer or network including school Wi-Fi without prior approval from the school IT Manager, with the exception of storage devices such as USB memory sticks. Approval will be based on the educational purpose or requirement of the individual.
- If you keep non-sensitive or non-personal data files on a personal storage device (such as a USB memory stick or external hard drive), you should ensure that other computers you connect this storage device to, (such as your own computers at home) has an up-to-date anti-virus system. All the latest operating system updates, and any third party software must be updated to the latest version, such as flash player. This is to protect against virus attacks on the school computer system. Advice on software is available from the school IT department.

Conduct

At all times, you must conduct your computer usage professionally, which includes being polite and using the system in a safe, legal and appropriate business-like manner.

The following uses are considered unacceptable:

- Using, transmitting or seeking inappropriate, offensive, pornographic, vulgar, obscene, abusive, harassing, threatening, racist, sexist or defamatory language or materials.
- Making ethnic, sexual-preference or gender-related slurs or jokes.
- You must respect, and not attempt to bypass, security or access restrictions in place on the computer system.
- You should not intentionally damage, disable or otherwise harm the operation of computers.
- You should make efforts to not intentionally waste resources. Examples of resource wastage include:
  - Excessive downloading of material from the Internet;
  - Excessive storage of unnecessary files on the network storage areas;
  - Excessive or personal streaming of video
  - Use of computer copiers to produce class sets of materials, instead of using reprographics.
- You should not eat or drink around computer equipment.
- All use of the Internet is governed by a legal agreement with our Internet Service Provider (ISP) in addition to the guidelines here.

Use of social networking sites, blogs, forums and non-school emails

(These guidelines apply to all current AND ex-students under 18 years of age). Staff must take care when using social networking websites such as Facebook, Instagram, Twitter etc. Social Networking sites promote informal relationships and increased sharing of personal information. As such, they can leave you open to abuse. In particular:

- You **must not** attempt to contact a student via any non-school resource.
- You **must not** allow any student to make contact with you via any non-school resource. Such attempts should be ignored and persistent attempts must be reported to the relevant member of staff in school. Also, note that people contacting you may not be who they say they are.
- You should take all reasonable steps to ensure that no personally identifying information is publicly available. You should set profiles so that only 'friends' can see such information. Be aware that services, such as Facebook, often allow 'friends of friends' to see such information and you should be cautious of anything you post online.
- You must not bring the school, or the teaching, or educational support profession into disrepute.

Staff should take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the school – even if their online activities are entirely unrelated to the school. This includes use of inappropriate language or discussion of unsuitable subject matters.

Additionally:

- Unless authorised to do so, you should not post content on websites that may appear as if you are speaking for the school.
- You should not post any material online that clearly identifies yourself, another member of staff, or a student, that could potentially be used to embarrass, harass, or defame the subject.
- You should not exchange personal contact methods (telephone numbers, personal email addresses, online username/nicknames (including gaming networks) etc.) with students for any reason.

Use of Email

All members of staff, with a computer account, are provided with an email address for communication both internally and with other email users outside the school. The following considerations must be made when communicating by email:

- Email has the same permanence and legal status as written hardcopy (paper) documents and may be subject to disclosure obligations in exactly the same way. Copies of emails, therefore, may have to be made available to third parties. You should be cautious when sending both internal and external mails. The professional standards that apply to internal memos and external letters must be observed for email.
- Email to outside organisations has the same power to create a binding contract as hardcopy documents. Check your email as carefully as if it were a written contract. Always use a spell checker and, where appropriate, obtain legal advice before sending. You may not purchase goods or services on behalf of the school, via email, without proper authorisation.
- All school email you send should have a signature containing your name, job title and the name of the school. Please see the school IT staff for help with this if required.
- Email is not a secure method of communication, and can be easily copied, forwarded and archived. Unless explicitly authorised to do so, you should not send, transmit, or otherwise distribute proprietary information, copyrighted material, trade secrets, or other confidential information belonging to the school.
- Having an external email address may lead to receipt of unsolicited email containing offensive and/or sexually explicit content. The school will take measures to minimise the receipt and impact of such content, but cannot be held responsible for material viewed, or received, from the Internet.
- You should not use the school email account to send private or personal messages, including signing up to sites or services that are not school related.
- You must not send chain letters or unsolicited commercial email (also known as SPAM). Microsoft have the rights to block future use of your email if your account is deemed as sending SPAM.

Supervision of Student Use

- Students should be supervised at all times when using school computer equipment. When arranging use of computer facilities for students, you must ensure supervision is available.
- Supervising staff are responsible for ensuring that the separate 'Responsible Use of the School ICT System' guidelines (Green Form) are enforced)

- Supervising staff should ensure that they have read and understood the separate guidelines on online safety, which pertains to the child protection issues of computer use by students.

Confidentiality and Copyright

- Respect the work and ownership rights of people outside the school, as well as other staff or students.
- You are responsible for complying with copyright laws and licenses that may apply to software, files, graphics, documents, videos, DVDs, messages, and other material you wish to use, download or copy. Even if materials on the school computer system or the Internet are not marked with the copyright symbol (©), you should assume that they are protected under copyright laws unless there is explicit permission on the materials to use them.
- You should consult the IT Manager before placing any order for computer hardware or software, or obtaining and using any software you believe to be free. This is to check that the intended use by the school is permitted under copyright law (as well as to check compatibility and discuss any other implications that the purchase/use may have). Do not rely on the claims of suppliers, who do not have specific knowledge of the school's system.

Reporting Problems with the computer System

It is the responsibility of the school IT department to ensure that the school computer system is working optimally at all times and that any faults are rectified as soon as possible.

- Please report any problems that need attention to a member of the school IT staff as soon as possible. Problems that seriously hinder your job or teaching and require immediate attention should be reported to the IT team by email/phone.
- If you suspect your computer has been affected by a virus/malware, or you receive spam or suspicious emails, please report this to a member of the school IT staff immediately.
- If you have lost documents or files, you should also report this as soon as possible. The longer a data loss problem goes unreported, the less the chance of your data being recoverable.

Privacy

- Use of the school computer system, including your email account and storage areas provided for your use, may be subject to monitoring by the school to ensure compliance of the Acceptable Use Policy and applicable laws. This may include remote monitoring of an interactive logon session. In particular, the school may keep a record of sites visited on the Internet by both students and staff. However, usernames and passwords used on those sites are not monitored or recorded.
- You should avoid storing sensitive personal information on the school computer system that is unrelated to school activities (such as personal passwords, photographs, or financial information). Use of the school computer system indicates your consent to the above monitoring taking place.
- Storage of any out-dated or no longer required information about staff or students, is a violation of the GDPR.

Reporting Breaches of this Policy

All members of staff have a duty to ensure the Acceptable Use Policy is followed. You should inform a member of the school IT department, Natalie Watson, or the headteacher, immediately, of abuse of any part of the computer system. In particular, you should report:

- any websites accessible from within school that you feel are unsuitable for staff or student consumption;
- inappropriate content suspected to be stored on the computer system. This may be contained in emails, documents, pictures, etc;

Declaration (returned by email and/or signature for supply staff)

Use of the school computer system indicates your agreement to this policy. If you do not agree to any part, please do not attempt to access the system. Instead, contact Ian Thompson/Natalie Watson as soon as possible.

Following your appointment, you will have been asked to sign an electronic declaration stating that you have read and agree with this policy. All staff are required to keep up-to-date with changes and will be asked to confirm agreement, and comply with any policy changes, on an annual basis.