Icknield Community College

Online Safety

(e-Safety) Policy

Icknield Community College

Approval & Review

Author:	Dr R Legg
Review Period:	Annually
Status of Policy:	Key Policy

Reviewed by (Committee):	Governing Body
Date of Review:	10 May 2022

Signed: David Marca .
(Chair of Governing Body)

Date of Next Review:	May 2023

Table of Contents

1. Policy aims

- Icknield Community College believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, mobile phones or games consoles.
- Icknield Community College views the Internet and information communication technologies as an important part of everyday life and believes that children must be supported to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.
- Icknield Community College has a duty to provide the school community with high quality Internet access to raise education standards, promote student achievement, support professional work of staff and enhance the school's management functions. Icknield Community College understands its corresponding duty to ensure that children are protected from potential harm online.
- The purpose of the Icknield Community College Online Safety (e-Safety) Policy is to:
  - clearly identify the key principles expected of all members of the community regarding the safe and responsible use of technology, to ensure that Icknield Community College is a safe and secure environment;
  - safeguard and protect all members of The school community online;
  - raise awareness among all members of the The school community regarding the potential risks as well as the benefits of technology;
  - enable all staff to work safely and responsibly, to model positive behaviour online, and to be aware of the need to manage their own standards and practices when using technology; and
  - establish and maintain clear procedures to use when responding to online safety concerns, and to ensure that these are known by all members of the community.
- Icknield Community College understands that risks relating to online safety can be broadly categorised in three areas:
  - **Content.** Exposure to illegal, inappropriate or harmful material.
  - **Contact.** Harmful online interaction with other users.
  - **Conduct.** Personal online behaviour that increases the likelihood of, or causes, harm.

1.2 Writing the online safety policy

- The Icknield Community College online safety policy has been written by the school, building on the Kent County Council online safety policy template with specialist advice and input as required.
- The policy has been approved and agreed by the Leadership Team and governing body.
- The School has appointed a member of the Governing Body to take lead responsibility for online safety (e-Safety).
- The school has appointed a member of the Leadership Team as the Online Safety Lead.

2. Policy scope

- Icknield Community College believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all students and staff are protected from potential harm online.
- Icknield Community College understands that the Internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- Icknield Community College believes that students should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as students, and parents and carers.
- This policy applies to all access to the Internet and use of information communication devices including personal devices or where students, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptop or mobile phone.

2.1 Links with other policies and practices

- This policy must be read in conjunction with other relevant school policies including (but not limited to):
  - Safeguarding and Child Protection
  - Anti-bullying
  - Behaviour and Engagement
  - Data Protection
  - Acceptable Use Policies
  - Relevant Curriculum policies including the Sex Education Policy.

3. Monitoring and review

- Icknield Community College will review this policy at least annually.
  - The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure
- We will ensure that we regularly monitor Internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure s/he has oversight of online safety, the Headteacher will be informed of online safety concerns, as appropriate.
- The named Governor for safeguarding will report on a regular basis to the governing body on online safety incidents, including outcomes.
- Any issues identified will be incorporated into the school's action planning.

4. Key responsibilities of the community

The School Online Safety (e-Safety) Coordinator is James Barringer.

The School Designated Safeguarding Lead (DSL) is Vicky Pickford.

Icknield Community College recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 Key responsibilities of the school's Leadership Team

- Developing an online safety culture, and promoting it to all stakeholders in line with national and local best practice recommendations, with appropriate support and consultation throughout the school community.
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.
- Supporting the online safety (e-Safety) lead in the development of an online safety culture within the setting.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety.
- Ensure that suitable and appropriate filtering and monitoring systems are in place.
- To ensure that suitable, age-appropriate and relevant filtering is in place to protect children from inappropriate content (including extremist material) to meet the needs of the school community and ensuring that the filtering and school network system is actively monitored.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is embedded within a progressive whole school curriculum which enables all students to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- Making appropriate resources available to support the development of an online safety culture.
- Taking responsibility for online safety incidents and liaising with external agencies as appropriate.
- Receiving and regularly reviewing online safety incident logs and using them to inform future practice.
- Ensuring there are robust reporting channels for the school to access regarding online safety concerns, including internal, local and national support.
- Ensuring that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- Working with and supporting technical staff in monitoring the safety and security of the school's systems and networks.
- Ensuring that the Designated Safeguarding Lead (DSL) works in partnership with the online safety (e-Safety) lead.

4.2 Key responsibilities of the Designated Safeguarding / Online Safety Lead

- Acting as a named point of contact on all online safety issues and liaising with other members of staff and agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends regarding online safety and communicating changes to the school community, as appropriate.
- Ensuring all members of staff receive appropriate online safety training.
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Working with the school lead for data protection and data security to ensure that practice is in line with legislation.
- Maintaining an online safety incident/action log to record incidents and actions taken as part of the school's safeguarding recording structures and mechanisms.
- Monitoring the school online safety incidents to identify gaps/trends and update the education response, policies and procedures.
- Reporting online safety concerns, as appropriate, to the school Leadership Team, Governing Body and other agencies.
- Liaising with the local authority and other local and national bodies as appropriate.
- Reviewing and updating online safety policies, Acceptable Use Policies (AUPs) and other procedures on a regular basis (at least annually) with stakeholder input.
- Ensuring that online safety is integrated with other appropriate school policies and procedures.
- Meeting regularly with the governor with a lead responsibility for online safety.

4.3 Key responsibilities of staff

- Contributing to the development of online safety policies.
- Reading the school Acceptable Use Policies (AUPs) and adhering to them.
- Taking responsibility for the security of school systems and data they use or have access to.
- Having an awareness of online safety issues, and how they relate to the children in their care.
- Modelling good practice in using new technologies and maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern, and taking appropriate action by working with the designated safeguarding lead.
- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Taking personal responsibility for professional development in this area.

4.4 Additional responsibilities for staff managing the technical environment (IT Services)

- Providing technical support and advice to the DSL and Leadership Team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implementing appropriate security measures (including password policies and encryption) to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, while allowing learning opportunities to be maximised.
- Ensuring that the school's filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the Leadership Team.
- Reporting any filtering breaches to the DSL and Leadership Team, as well as the school's Internet Service Provider or other services, as appropriate.
- Ensuring that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the school's safeguarding procedures.

4.5 Key responsibilities of students (at a level that is appropriate to their individual age, ability and vulnerabilities)

- Engaging in age-appropriate online safety education opportunities.
- Contributing to the development of online safety policies.
- Reading the school Acceptable Use Policy (AUP) and adhering to it.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.
- Taking responsibility for keeping themselves and others safe online.

4.6. Key responsibilities of parents and carers

- Reading the school Acceptable Use Policy, encouraging their children to adhere to it, and adhering to it themselves where appropriate.
- Discussing online safety issues with their children, supporting the school in its online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Modelling safe and appropriate uses of new technology and social media.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Using school systems, such as learning platforms, and other network resources, safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

5. Online communication

5.1 Managing the school website

- The school will ensure that information posted on the school website meets the requirements laid out by the Department for Education.
- The contact details on the website will be the school address, email and telephone numbers. Staff or students' personal information will not be published.
- The Headteacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including: respect for intellectual property rights; accessibility; data protection; privacy policies and copyright.
- Students' work will only be published with their permission and/or that of their parents and carers.
- The administrator account for the school website will be secured with an appropriately strong password.
- The school will post information about safeguarding, including online safety, on the school website.

5.2 Publishing images and videos online

- The school will ensure that all images are used in accordance with the school image use policy.
- In line with the school's image policy, written permission from parents or carers will always be obtained before images/videos of students are electronically published.

5.3 Managing email

- Access to school email systems will always take place in accordance with data protection legislation and in line with other school policies, including: Confidentiality, AUP and Code of Conduct.

    - The forwarding of any chain messages/emails is not permitted. Spam or junk mail will be blocked and reported to the email provider.
    - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
    - School email addresses and other official contact details will not be used for setting up personal social media accounts.

- Members of the school community will immediately tell the DSL, Vicky Pickford, if they receive offensive communication, and this will be recorded in the school safeguarding files/records.

- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked in school.
- The school will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.

5.3.1 Staff

- Email sent to external organisations should be written carefully, in the same way as a letter written on school headed paper would be.
- All members of staff are provided with a specific school email address to use for any official communication.
- The use of personal email addresses by staff for any official school business is not permitted.
- Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and encrypted methods.

5.3.2 Students

- Students may only use school provided email accounts for educational purposes.
- Students will sign an AUP and will receive education regarding safe and appropriate email etiquette before access is permitted.

6. Safer use of technology

6.1 Appropriate and safe classroom use of the Internet and associated devices

- Icknield Community College uses a wide range of technology. This includes:
    - computers, laptops and other digital devices
    - Internet which may include search engines and educational websites
    - school learning platform/intranet
    - email
    - games consoles and other-games based technologies
    - digital cameras, web cams and video cameras

- All school-owned devices will be used in accordance with the school’s Acceptable Use Policy and with appropriate safety and security measures in place.
    - All devices have their Internet connection filtered and monitored through the school’s Smoothwall filtering system.
    - All Windows devices are monitored through a SECURUS system.
    - Tablets are added to the school’s Lightspeed MDM solution.
- The school’s Internet access will be designed to enhance and extend education.

- Access levels to the Internet will be reviewed to reflect the curriculum requirements and the age and ability of students.
- The school will use age-appropriate search tools, specifically Google Safe Search, following an informed risk assessment, to identify which tool best suits the needs of our community.
- Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum.
- The school will ensure that the use of Internet-derived materials by staff and students complies with copyright law and acknowledge the source of information.
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- Supervision of students will be appropriate to their age and ability; students will be appropriately supervised when using technology, according to their ability and understanding.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will use the Internet to enable students and staff to communicate and collaborate in a safe and secure environment.
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

6.2 Management of school learning platforms (LP), portals & gateways

The school's Network Manager will monitor the usage of LPs by students and staff in all areas, in particular message and communication tools and publishing facilities.

- Students and staff will be advised about acceptable conduct and use when using LPs.
- Only members of the current students, parent/carers and staff community will have access to LPs.
- All users will be mindful of copyright issues and will only upload appropriate content onto LPs.
- When staff, students, etc., leave the school their accounts and/or rights to specific school areas will be disabled or transferred to their new establishment.
- Any concerns about content on LPs may be recorded and dealt with in the following ways:

a) The user will be asked to remove any material deemed to be inappropriate or offensive.
b) The material will be removed by the site administrator if the user does not comply.
c) Access to LPs for the user may be suspended.

d) The user will need to discuss the issues with a member of leadership before reinstatement.
e) A student's parent/carer may be informed.

- A visitor may be invited onto the LP by a member of the leadership. In this instance there may be an agreed focus or a limited time slot.
- Students may require editorial approval from a member of staff. This may be given to the student to fulfil a specific aim and may have a limited time frame.

6.3 Authorising Internet access

- The school will maintain a current record of all staff and students who are granted access to the school's electronic communications.
- All staff, students and visitors will read and sign the school's Acceptable Use Policy before using any school ICT resources.
- Parents will be informed that students will be provided with supervised Internet access which is appropriate to their age and ability.
- Parents will be asked to read the school's Acceptable Use Policy and to discuss it with their child, where appropriate.
- When considering access for vulnerable members of the school community (such as with students with special education needs) the school will make decisions based on the specific needs and understanding of the individuals.

6.4 Filtering and monitoring

6.4.1 Decision making

- The school's Internet access strategy will be dependent on the needs and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our students, with advice from technical, educational and safeguarding staff.
- The school will ensure that age- and ability-appropriate filtering is in place while using school devices and systems to try to prevent staff and students from being accidentally or deliberately exposed to unsuitable content.
- Changes to the school filtering policy will be risk-assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Leadership Team.
- All changes to the school filtering policy will be logged and recorded.
- The Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.

6.4.2 Filtering

- The school uses educational filtered secure broadband connectivity through RM Education, which is appropriate to the age and requirement of our students.
- The school uses Smoothwall filtering system which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.
- The sfiltering system blocks all sites on the Internet Watch Foundation (IWF) list.
- The school will work with RM and Smoothwall to ensure that filtering policy is continually reviewed.

6.4.3 Dealing with filtering breaches

- The school has a clear procedure for reporting breaches of filtering.
  - If students discover unsuitable sites, they will be required to turn off the monitor/screen and report the concern immediately to a member of staff
  - The member of staff will report the concern (including URL of the site is possible) to the Designated Safeguarding Lead and/or technical staff.
  - The breach will be recorded and escalated as appropriate.
  - Parent/carers will be informed of filtering breaches involving their child.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Thames Valley Police or CEOP (Child Exploitation and Online Protection) immediately.

6.4.4 Monitoring

- The school will appropriately monitor Internet use on all school-owned or -provided Internet enabled devices. This is achieved by:
  - physical monitoring (supervision);
  - monitoring Internet and web access via logfiles and reports;
  - active technology monitoring services, such as Securus.
- The school has a clear procedure for responding to concerns identified via monitoring approaches.
  - DSL will respond in line with the child protection policy
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

6.5 Managing personal data online

- Personal data will be recorded, processed, transferred and made available online in accordance with the Data Protection Act 1998.

7. Social media

7.1. Expectations

- Expectations regarding safe and responsible use of social media will apply to all members of the school community and exist in order to safeguard both the school and the wider community, on and offline.
- Examples of social media may include (but is not limited to): blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms and instant messaging services.
- All members of the school community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
  - All members of the school community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the school community.
- The school will control student access to social media and social networking sites while on site and using school provided devices and systems. Student access will be blocked through our filtering system, Smoothwall.

  - The use of social networking applications during school hours for personal use is not permitted for students.
  - Inappropriate or excessive use of social media during school hours or while using school devices may result in disciplinary or legal action and/or removal of Internet facilities.

- Any concerns regarding the online conduct of any member of the school community on social media sites should be reported to the school Leadership Team and will be managed in accordance with existing school policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.
- Any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with the relevant school policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

7.2 Official use of social media

- Icknield Community College's official media channels are:
  - Twitter - https://twitter.com/IcknieldCC
  - Facebook - https://www.facebook.com/IcknieldCC
  - Youtube - https://www.youtube.com/user/IcknieldCC

- Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
    - Official use of social media sites as communication tools will be risk assessed and formally approved by the Headteacher.
    - Leadership staff must be aware of account information and relevant details for social media channels in case of emergency such as staff absence.
- Official school social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes.
    - Staff will use school provided email addresses to register for and manage official school approved social media channels.
    - Official social media sites are suitably protected and, where appropriate and possible, run and/or linked to the school website.
- Members of staff running official school social media channels will sign a specific Acceptable Use Policy (AUP) to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
- All communication on official school social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official school social media sites will comply with legal requirements including the General Data Protection Regulation 2016/679, the right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
- Official social media use by the school will be in line with existing policies including anti-bullying and child protection.
- Images or videos of children will only be shared on official school social media sites/channels in accordance with the school image use policy.
- Information about safe and responsible use of school social media channels will be communicated clearly and regularly to all members of the school community.
- Parents and carers, and students, will be informed of any official school social media use, along with expectations for safe use and school action taken to safeguard the community.
- The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.
- Parents will be informed of any official social media use with students and written parental consent will be obtained, as required.

7.3 Staff official use of social media

- Members of staff who follow and/or like the school social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online activity as part of their capacity as an employee of the school, they will:

- be professional at all times and that they are an ambassador for the school;
- disclose their official role/position but always make it clear that they do not necessarily speak on behalf of the school;
- be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared;
- act within the legal frameworks they would adhere to within school, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws;
- ensure that any image posted on the school social media channel have appropriate written parental consent;
- be accountable and not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so;
- inform their line manager, the school online safety (e-Safety) lead and/or the Headteacher of any concerns such as criticism or inappropriate content posted online;
- not engage with any direct or private messaging with students or parents and carers through social media and should communicate via school communication channels; and
- sign the school social media Acceptable Use Policy before any official social media use takes place.

7.4 Staff personal use of social media

- Personal use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Acceptable Use Policy.

Communicating with students and parents and carers

- All members of staff are advised not to communicate with or add as ‘friends’ any current or past students or current or past students’ family members via any personal social media sites, applications or profiles.
  - Any pre-existing relationships or exceptions that may compromise this will be discussed with line manager, member of Leadership Team, or Headteacher.
  - If ongoing contact with students is required once they have left the school roll, then members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- All communication between staff and members of the school community on school business will take place via official approved communication channels (such as school email address or phone numbers). Staff must not use personal accounts or information to make contact with students or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher or line manager.

- Any communication from students/parents received on personal social media accounts will be reported to the school's designated safeguarding lead.
- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within and beyond the school. Civil, legal or disciplinary action may be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- Information staff members have access to as part of their employment, including photos and personal information about students and their family members, colleagues, etc. will not be shared or discussed on personal social media sites.
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to consider carefully the information, including text and images, they share and post online and should ensure that their social media use is compatible with their professional role, in accordance with school's policies (safeguarding, confidentiality, data protection etc.) and the wider professional and legal framework.
- Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites, conflicts with their role in the school.
- Members of staff are encouraged not to identify themselves as employees of Icknield Community College on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members and the wider school community.
- Member of staff will ensure that they do not represent their personal views as that of the school on social media.
- School email addresses will not be used for setting up personal social media accounts.
- Members of staff who follow/like the school's social media channels will be advised to use dedicated professional accounts where possible to avoid blurring professional boundaries.

7.5 Students' use of social media

- Safe and responsible use of social media sites will be taught to students as part of an embedded and progressive educational approach, via age-appropriate sites and resources.
- Personal publishing on social media sites will be taught to students as part of an embedded and progressive educational approach via age-appropriate sites which have been risk-assessed and approved as suitable for educational purposes.
- Students will be advised:
    - To consider the risks of sharing personal details of any kind on social media sites which may identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, instant messaging service contact details, email addresses, full names of friends/family, specific interests and clubs, etc.
    - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when such a responsible person can be present.
    - About appropriate security on social media sites, and will be encouraged to use safe and secure passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
    - To approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.

- Any official social media activity involving students will be moderated by the school where appropriate.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts specifically for children under this age.
- Any concerns regarding students' use of social networking, social media and personal publishing sites, either at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will be raised with their parents and carers, particularly when concerning any underage use of social media sites.

8. Use of personal devices and mobile phones

- Icknield Community College recognises that personal communication through mobile technologies is an accepted part of everyday life for students, staff, and parents and carers but requires that such technologies need to be used safely and appropriately within school.

8.1 Expectations

- The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members of the school community to take steps to ensure that mobile phones and personal devices are used responsibly.

- The in-school use of mobile phones and other personal devices by young people and adults will be decided by the school and covered in appropriate policies including, but not limited to: Anti-bullying, Behaviour, Child Protection and the school Acceptable Use Policy.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user at all times.
    - All members of Icknield Community College are advised to take steps to protect their mobile phones and other devices from loss, theft or damage; the school accepts no responsibility for the loss, theft or damage of such items, nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
    - All members of the school community are advised to use passwords and/or PINs to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and PINs should be kept confidential, and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms and toilets.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches while on school premises will be dealt with as part of the school behaviour and engagement policy.
- Members of staff will be issued with a work phone number and email address where contact with students or parents and carers is required.
- All members of the school community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school/settings policies.
- School mobile phones and devices must always be used in accordance with the Acceptable Use Policy
- School mobile phones and devices used for communication with parents and students must be suitably protected using a passcode, password or PIN and must only be accessed and used by members of staff.

8.2 Students’ use of personal devices and mobile phones

- Students will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- All use of mobile phones and personal devices by children will take place in accordance with the AUP.
- Mobile phones or personal devices will not be used by students during lessons or formal school time unless as part of an approved and directed curriculum-based activity with the permission of a member of staff.
    - The use of personal mobile phones or devices for a specific education purposes does not mean that blanket use is authorised.
- If a student needs to contact his/her parents and carers s/he will be allowed to use a school phone.

- Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office. Exceptions may be permitted in exceptional circumstances on a case-by-case basis and as approved by the Headteacher.

- Students should protect their phone numbers by only giving them to trusted friends and family members.
- Phones and devices must not be taken into examinations.
    - Students found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from that examination or from all examinations.
- If a student breaches the school policy then the phone or device can be confiscated by the teacher or adult supervising.
    - School staff may confiscate a student's mobile phone or device if they believe it is being used to contravene the school's behaviour or bullying policy, or could contain youth produced sexual imagery (sexting).
    - It will be returned to the student at a time deemed appropriate.
- If there is suspicion that material on a student's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence then the device will be handed over to the police for further investigation.

8.3 Staff use of personal devices and mobile phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant school policy and procedures, such as: Confidentiality, Child protection, Data Security and Acceptable Use Policy.
- Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside the setting in a professional capacity, except in some circumstances, such as some educational visits, as agreed by the Headteacher.
    - Any pre-existing relationships which could compromise this principle must be discussed with leaders/managers.
- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of students except where this is required and agreed, for example in order to illustrate good work. In such cases, appropriate passwords, passcodes or PINs should be in place to prevent inappropriate use in the event of a device being lost or stolen.
- Staff will be advised to:
    - Keep staff personal mobile phones and devices switched off/switched to 'silent' mode during lesson times.
    - That personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.
    - Ensure that any content bought on site via mobile phones and personal devices is compatible with their professional role and expectations.
    - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.

- If a member of staff breaches the school policy then disciplinary action will be taken.
    - If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device, or to have committed a criminal offence, then the police will be contacted and allegations will be responded to following the Staff Allegations Policy.

8.4 Visitors' use of personal devices and mobile phones

- Parents and carers and visitors must use mobile phones and personal devices in accordance with the school's policy.
- Use of mobile phones or personal devices by visitors and parents and carers to take photos or videos must take place in accordance with the school image use policy.
- The school will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

8.5 Officially provided mobile phones and devices

- Members of staff will be issued with a work phone number and email address, where contact with students or parents and carers is required.
- School mobile phones and devices will be suitably protected via a passcode, password or PIN and must only be accessed or used by members of staff.
- School mobile phones and devices will always be used in accordance with the Acceptable Use Policy and other relevant policies.

9. Engagement approaches

9.1 Engagement and education of children and young people

- An online safety (e-Safety) curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible Internet use amongst students.
- Education about safe and responsible use will precede Internet access.
- Students' input will be sought when writing and developing school online safety policies and practices through student voice.
- Students' will be supported in reading and understanding the school Acceptable Use Policy in a way which suits their age and ability.
- All users will be informed that network and Internet use will be monitored, including https traffic.
- Online safety (e-Safety) will be included in the PSHCE, Citizenship and Computing programmes of study covering both safe school and home use.

- Online safety (e-Safety) education and training will be included as part of the transition programme across the Key Stages and when moving between establishments.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.
- External support will be used to complement and support the school's internal online safety (e-Safety) education approaches.
- The school will implement peer education to develop online safety as appropriate to the needs of the students.
- Educating students in the effective use of the Internet to research; including the skills of knowledge location, retrieval and evaluation.

9.1.1 Engagement and education of children and young people who are considered to be vulnerable

- Icknield Community College is aware that some children may be considered to be more vulnerable online due to a range of factors and will ensure that differentiated and ability appropriate online safety (e-Safety) education is given, with input from specialist staff as appropriate (e.g. SENCO).

9.2 Engagement and education of staff

- The online safety (e-Safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of school safeguarding practice.
- To protect all staff and students, the school will implement Acceptable Use Policies which highlights appropriate online conduct and communication.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and appropriate professional conduct are essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff on a regular basis.
- The school will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the students.
- All members of staff will be made aware that their online conduct outside school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff will be made aware of the procedures to follow regarding online safety concerns affecting students, colleagues or other members of the school community.

9.3 Engagement and education of parents and carers

- Icknield Community College recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the Internet and digital technology.
- Parents' attention will be drawn to the school online safety (e-Safety) policy and expectations in newsletters, letters 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 parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well-attended events e.g. parents' evenings, transition events, fetes and sports days.
- Parents will be encouraged to read the school Acceptable Use Policy for students and discuss its implications with their children.
- Information and guidance for parents on online safety will be made available to parents in a variety of formats.
- Parents will be encouraged to model positive behaviour for their children online.

10. Managing information systems

10.1 Security and management of information systems

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.
- Portable media may not be used without specific permission followed by an anti-virus / malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- The network manager will review system capacity regularly.
- The appropriate use of user logins and passwords to access the school network will be enforced for all.
- Staff users will be expected to log off or lock their screens/devices if systems are unattended.
- The school will log and record Internet use on all devices connected to the school's network.

10.2 Password policy

- All users will be informed not to share passwords or information with others and not to log in as another user at any time.
- Staff and students must always keep their passwords private and must not share them with others or leave them where others can find it.
- All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their passwords private.
- All students are provided with their own unique username and private passwords to access school systems. Students are responsible for keeping their passwords private.

10.3 Management of applications (apps) used to record children's progress

The school uses SIMS.net to track students' progress and share appropriate information with parents and carers.

- The Headteacher is ultimately responsible for the security of any data or images held relating to students. S/he will ensure that the use of tracking systems is appropriately risk-assessed prior to use, and that they are used in accordance with data protection.
- In order to safeguard students' data:
  - Personal staff mobile phones or devices will not be used for any apps which record and store students' personal details, attainment or photographs.
  - Only school-issued devices will be used for apps that record and store children's personal details, attainment or photographs, other than in cases described in 8.3 above.
  - Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.
  - Staff, parents and carers will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.

11. Responding to online incidents and concerns

- All members of the school community will be informed about the procedure for reporting online safety (e-Safety) concerns including, breaches of filtering, youth-produced sexual imagery (sexting), cyberbullying and illegal content.
- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Complaints about online bullying will be dealt with under the School's anti-bullying policy and procedures.
- All members of the school community need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
  - Students, parents and staff will be informed of the school's complaints procedure and staff made aware of the whistleblowing procedure.

- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- The school will manage online safety (e-Safety) incidents in accordance with the school behaviour policy, where appropriate.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Education Safeguarding Team or Thames Valley Police via 999 if there is immediate danger or risk of harm.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Thames Valley Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.
- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the Education Safeguarding Team to communicate to other schools/settings in the area.
- Parents and children will need to work in partnership with the school to resolve online safety issues.

11.1 Concerns about students' welfare

- The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns. The DSL will record these issues in line with the school's child protection policy.
- The Designated Safeguarding Lead (DSL) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Oxfordshire Safeguarding Children Board thresholds and procedures.
- The school will inform parents and carers of any incidents of concerns as and when required.

11.2 Staff misuse

- Any complaint about staff misuse will be referred to the Headteacher.

- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with the Behaviour Policy and Code of Conduct.

12. Reducing online risks

Icknield Community College is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace. We will:

- Ensure that emerging technologies will be examined for educational benefit. The school's Leadership Team will ensure that appropriate risk assessments are carried out before use in school is allowed.
- Ensure that appropriate filtering systems are in place to prevent staff and students from accessing unsuitable or illegal content.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, owing to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer or device.
- The school will audit technology use to establish if the online safety (e–Safety) policy is adequate and that the implementation of the policy is appropriate.
- Methods to identify, assess and minimise online risks will be reviewed regularly by the school's Leadership Team.
- Filtering decisions, Internet access and device use by students and staff will be reviewed regularly by the school's Leadership Team.

The school will provide an Acceptable Use Policy for any guest/visitor who needs to access the school computer system or Internet on site.

13. Procedures for responding to specific online incidents or concerns

The following content is provided to enable schools and education settings to make appropriate safeguarding decisions reading online safety concerns and has been adapted from materials written by the Kent e-Safety Strategy Group with input from specialist services and teams. This content is not exhaustive and cannot cover every eventuality so professional judgement and support from appropriate agencies such as the Education Safeguarding Team, Police, CSET and Children's Social Care is encouraged.

13.1 Youth-produced sexual imagery or "sexting"

- Icknield Community College ensures that all members of the community are made aware of the social, psychological and criminal consequences of sharing, possessing and creating incident images of children (known as "sexting").
- The school will implement preventative approaches via a range of age and ability appropriate educational approaches for students, staff, and parents and carers.

- Icknield Community College views “sexting” as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead: Vicky Pickford, Deputy Headteacher.
- The school will ensure that all members of the community are aware of sources of support regarding youth-produced sexual imagery.

13.2 Dealing with ‘sexting’

- If the school are made aware of incident involving the creation or distribution of youth produced sexual imagery, the school will:

  - Act in accordance with the school’s Child Protection and Safeguarding Policy and the relevant Oxfordshire Safeguarding Child Board’s procedures.
  - Immediately notify the Designated Safeguarding Lead.
  - Store the device securely.
  - If an indecent image has been taken or shared on the school network or devices, the school will block access to all users and isolate the image.
  - Carry out a risk assessment in relation to the children(s) involved.
  - Consider the vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies)
  - Inform parents and carers, if appropriate, about the incident and how it is being managed.
  - Make a referral to children’s social care and/or the police (as appropriate).
  - Put the necessary safeguards in place for students e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
  - Implement appropriate sanctions in accordance with the school’s behaviour policy but taking care not to further traumatise victims where possible.
  - Consider the deletion of images in accordance with the UKCCIS: ‘Sexting in schools and colleges: responding to incidents and safeguarding young people’ guidance. Images will only be deleted once the school has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation
  - Review the handling of any incidents to ensure that the school is implementing best practice and the Leadership Team will review and update any management procedures where necessary.

- The school will not:

  - View the image unless there is a clear need or reason to do so.
  - Share or save indecent images of children.
  - Allow or request children to share or save indecent images of children.

- The school will need to involve or consult the police if images are considered to be illegal.

- The school will take action regarding indecent images, regardless of the use of school equipment or personal equipment, both on and off the premises.
- The school will follow the guidance (including the decision-making flow chart and risk assessment template) as set out in "'Sexting' in schools: advice and support around self-generated images. What to do and how to handle it".

13.2. Online child sexual abuse and exploitation

- Icknield Community College ensures that all members of the community are aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for students, staff, and parents and carers.
- Icknield Community College views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead: Vicky Pickford, Deputy Headteacher.
- The school will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
- The school will ensure that the Click CEOP report button is visible and available to students and other members of the school community, for example the CEOP report button is an icon on the school's RM Unify homepage, which is the students' homepage.

13.2.1 Dealing with online child sexual abuse and exploitation

- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Thames Valley Police.
- If the school are made aware of incident involving online child sexual abuse of a child then the school will:
    - Act in accordance with the school's Child Protection and Safeguarding Policy and the relevant Oxfordshire Safeguarding Child Board's procedures.
    - Immediately notify the designated safeguarding lead.
    - Store any devices involved securely.
    - Immediately inform Thames Valley Police via 101 (using 999 if a child is at immediate risk).
    - Carry out a risk assessment which considers any vulnerabilities of student(s) involved (including carrying out relevant checks with other agencies).
    - Make a referral to children's social care (if needed/appropriate).
    - Put the necessary safeguards in place for student(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
    - Inform about the incident and how it is being managed.

  - Review the handling of any incidents to ensure that the school is implementing best practice and the school Leadership Team will review and update any management procedures where necessary.
- The school will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.
    - Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse such as via the Click CEOP report form: http://www.ceop.police.uk/safety-centre/
- If students at other schools are believed to have been targeted then the school will seek support from the Education Safeguarding Team to enable other schools to take appropriate action to safeguard their community.
- If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the Designated Safeguarding Lead.

13.3. Responding to concerns regarding indecent images of children (IIOC)

- Icknield Community College will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.
- The school will take action regarding Indecent Images of Children (IIOC) regardless of the use of school equipment or personal equipment, both on and off the premises.
- The school will take action to prevent accidental access to Indecent Images of Children (IIOC) for example using an Internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, firewalls and anti-spam software.
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Thames Valley Police.

- If the school is made aware of Indecent Images of Children (IIOC) then the school will:
  - Act in accordance with the school's Child Protection and Safeguarding Policy and the relevant Oxfordshire Safeguarding Child Board's procedures.
  - Immediately notify the school Designated Safeguard Lead.
  - Store any devices involved securely.
  - Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF), Thames Valley Police via 101 (using 999 if a child is at immediate risk) and/or the LADO (if there is an allegation against a member of staff).

- If the school is made aware that a member of staff or a student has been inadvertently exposed to indecent images of children while using the Internet then the school will:
  - Ensure that the Designated Safeguard Lead is informed.

  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Report concerns, as appropriate, to parents and carers.

- If the school is made aware that indecent images of children have been found on the school's electronic devices then the school will:
  - Ensure that the Designated Safeguard Lead is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
  - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
  - Report concerns, as appropriate, to parents and carers.

- If the school is made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:
  - Ensure that the Headteacher is informed in accordance with the school whistleblowing procedure.
  - Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the school's managing allegations policy.
  - Quarantine any devices until police advice has been sought.
  - Follow the appropriate school policies regarding conduct.

13.4. Online radicalisation or extremism

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the Internet in school and that suitable filtering is in place which takes into account the needs of students.
- When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the school safeguarding policy.
- If the school is concerned that a member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately and action will be taken in line with the Child protection and Allegations policies.

13.5 Cyberbullying

- Cyberbullying, along with all other forms of bullying, of any member of the school community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.

- All incidents of online bullying reported will be recorded.
- There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Thames Valley Police.
- Students, staff, and parents and carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Students, staff, and parents and carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.
- Sanctions for those involved in online or cyberbullying may include:
    - Those involved will be asked to remove any material deemed to be inappropriate or offensive.
    - A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
    - Internet access may be suspended at school for the user for a period of time. Other sanctions for students and staff may also be used in accordance to the school's anti-bullying, behaviour policy or Acceptable Use Policy.
    - Parent/carers of students involved in online bullying will be informed.
    - The police will be contacted if a criminal offence is suspected.

13.6 Online hate

- Online hate content, directed towards or posted by, of any member of the school community will not be tolerated and will be responded to in line with existing school policies, including anti-bullying and behaviour.
- There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online hate.
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Thames Valley Police.
- Students, staff, and parents and carers will be advised to report online hate in accordance with relevant school policies and procedures..

14. Acceptable use agreement: students

- I will only use ICT systems during directed school time, including the Internet, e-mail, digital video and mobile technologies for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network, other systems and resources with my own user name and password.
- I will follow the school's ICT security system and not reveal my passwords to anyone and change them regularly.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- Images of students and/ or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without the permission of the Headteacher.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring into disrepute.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the Internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer may be contacted.

15. Acceptable use agreement: staff, governors and visitors

ICT (including data) and the related technologies such as e-mail, 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 adhere at all times to its contents. Any concerns or clarification should be discussed with James Barringer, the school's Online Safety Coordinator.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to students.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of software without permission of the Network Manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images 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 Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- 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 Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help students to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

Each time students log in to a school machine or access the school's WIFI on their own personal device they are required to agree to the acceptable use agreement. This agreement will also be shared with parents periodically in the school's Newsletter so that the expectations of students are clear.

Similarly, each time staff, governors and visitors log on to a school machine or access WIFI through their own device, they will be required to agree to the acceptable use agreement.