Chilton Academy

'Chilton Academy & Nursery – where everyone C.A.N.'

Online Safety Policy
And
Acceptable Use Agreement

2019-2020

It is a primary aim of our academy that every member of the community feels happy, valued and respected, and that each person is treated fairly and well. We are a caring community with mutual trust and respect for all.

This policy should be read in conjunction with the Inclusion Policy, Rights Respecting Policy, Developing Positive Relationships Policy, Online Safety, Anti Bullying, all relevant guidance from the DfE as well as the 'Keeping children safe in education' (changes for Sept 2019).

ONLINE SAFETY POLICY

At Chilton Academy, we believe it is important that the rights of our children are protected and fully supported by all members of staff. This policy takes into consideration these rights and in particular *Article 13 (Freedom of expression): Children have the right to get and share information, as long as the information is not damaging to them or others.* In exercising the right to freedom of expression, children have the responsibility to also respect the rights, freedoms and reputations of others. Also, according to *Article 24 – children have the right to a safe environment.* This includes online and by agreeing to and following an acceptable use policy, the children are keeping themselves and their peers safe.

Introduction:

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our children with the skills to access life-long learning and employment. Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast-paced evolution of ICT within our society as a whole.

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.
At Chilton Academy we understand the responsibility to educate our pupils in online issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.
This policy is inclusive of both fixed and mobile internet, technologies provided by the school (such as PCs, laptops, tablets, webcams, whiteboards, digital video equipment, etc) and technologies owned by pupils and staff, but brought onto school premises (such as laptops, tablets, mobiles phones, camera phones and portable media players, etc).

Teaching and Learning:

Internet use is part of the statutory curriculum and is a necessary tool for learning. In today's society, the Internet is a part of everyday life for education, business and social interaction. Chilton Academy has a duty to provide students with quality Internet access as part of their learning experience. Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security. The purpose of Internet use in the academy is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the academy's management functions. Internet access is an entitlement for students who show a responsible and mature approach to its use. Therefore, developing effective practice in using the Internet for teaching and learning is essential.

Internet use will enhance learning:

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with DCC and DfE;
- access to learning wherever and whenever convenient.
- The academy will provide opportunities within a range of curriculum areas to teach online.
- Educating pupils on the dangers of technologies that may be encountered outside of the academy is done when opportunities arise and as part of the online curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- New filtering has been sourced to allow age appropriate accessibility.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use, guiding the pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Pupils will be taught how to evaluate Internet content:

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation.

- The academy will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to use search engines appropriately for their age.
- 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.

Roles and Responsibilities:

As online safety is an important aspect of strategic leadership within the academy, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named online co-ordinator in our school is Ms F. Brady; all members of the academy community are aware of who holds this post. The Online coordinator updates Senior Management and Governors and all governors have an understanding of the issues at our academy in relation to local and national guidelines and advice. The academy has appointed a member of the Governing Body, A.Coulthard, to take lead responsibility for online safety.

Relevant Responsible Persons

Senior members of staff should be familiar with information risks and the academy's response.

- they lead on the information risk policy and risk assessment
- they advise school staff on appropriate use of school technology
- they act as an advocate for information risk management

Information Asset Owner (IAO)

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. A responsible member of staff should be able to identify across the academy:

- what information is held, and for what purposes
- what information needs to be protected how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed of

As a result, this manager is able to manage and address risks to the information and make sure that information handling complies with legal requirements. However, it should be clear to all staff that the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

Monitoring

Authorised IT staff may inspect any IT equipment owned or leased by the academy at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any IT authorised staff member will be happy to comply with this request. IT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account. Through the use of the recently installed Smoothwall, the headteacher will also receive regular reports showing internet based searches and any items which have been deemed inappropriate. The headteacher can also access information regarding internet use of any member of staff using academy owned devices. All monitoring, surveillance or investigative activities are conducted by IT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Breaches

A breach or suspected breach of policy by an academy employee, contractor or pupil may result in the temporary or permanent withdrawal of school IT hardware, software or services from the offending individual. Any policy breach is grounds for disciplinary action in accordance with the academy Disciplinary Procedure or, where appropriate, the HCC Disciplinary Procedure or Probationary Service Policy.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the academy's SIRO or Online Safety Co-coordinator (Fiona Brady). Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your Senior Information Risk Owner who is Mrs. A. Pybus. These will then be logged on the incident reporting form and will be dealt with following the academy's related policies.

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using academy provided anti-virus software before being used.
- Never interfere with any anti-virus software installed on academy ICT equipment.
- If your machine is not routinely connected to the academy network, you must make provision for regular virus updates through your IT team.
- If you suspect there may be a virus on any academy ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know. (Academy technicians – GH / MW).

Password and Password Security

- Always use your own personal passwords
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- Only disclose your personal password to authorised ICT support staff when necessary - and never to anyone else.
- Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- Never tell a child or colleague your password
- If you aware of a breach of security with your password or account inform Mrs. F. Brady or Mrs. A. Pybus immediately
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols
- User ID and passwords for staff and pupils who have left the academy are removed from the system within 3 years (in accordance with County guidelines).

If you think your password may have been compromised or someone else has become aware of your password report this to your ICT support team.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords private and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the academy's e-Safety Policy and Data Security.

Personal or Sensitive Information

- Ensure that any school information accessed from your own PC or removable media equipment is kept secure and remove any portable media from computers when not attended.
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access.
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others.
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person.
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared copiers are used and when access is from a non-school environment.

- Only download personal data from systems if expressly authorised to do so by your manager.
- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience.
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labelling.

Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

All documentation should be accessed through the Google drive and no sensitive data should be removed from the academy premises using removable media. If in the event this is not possible, staff should:

- Ensure removable media is purchased with encryption
- Store all removable media securely
- Securely dispose of removable media that may hold personal data
- Encrypt all files containing personal, sensitive, confidential or classified data
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean Security
- The school gives relevant staff access to its Management Information System, with a unique username and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing academy data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- Staff keep all academy-related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used.

How will information systems security be maintained?

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils. ICT security is a complex issue which cannot be dealt with adequately within this document. A number of agencies can advise on security including DCC and network suppliers. Virus protection will be updated regularly. The school will comply with the terms of the data protection act, and is responsible for registering with the information commissioner's office . www.ico.gov.uk advice is available from www.ico.gov.uk/for_organisations/sector_guides/education.aspx

- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not used without specific permission followed by an antivirus / malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the academy's network will be regularly checked.
- The network manager will review system capacity regularly.
- The use of user logins and passwords to access the academy network will be enforced.

How should Web site content be managed?

• The point of contact on the Web site should be the academy address, school e-mail and telephone number. Staff or pupils' home or personal information will not be published.
• Web site photographs that include pupils will be selected carefully to comply with the Eden Learning Trust consent forms.
• Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
• Written permission from parents or carers will be obtained before photographs of pupils are published on the academy Web site or shared on Twitter. This is done through the academy photographic policy and parents provide permissions for their child each academic year.
• The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
• The Web site should comply with the academy's guidelines for publications.
• The copyright of all material must be held by the academy, or be attributed to the owner where permission to reproduce has been obtained.
• The academy will scan regularly their own web site to check links that have been made into their own sites and to remove links from potentially dangerous sources.

How will pupils' images or work be published?

Still and moving images and sound add liveliness and interest to a publication, particularly when pupils can be included. Nevertheless, the security of staff and pupils is paramount. Although common in newspapers, the publishing of pupils' names with their images is not acceptable. Published images could be reused, particularly if large images of individual pupils are shown. "Over the shoulder" can replace "passport style" photographs but still convey the educational activity. Personal photographs can be replaced with self-portraits or images of pupils' work or of a team activity. Pupils in photographs should, of course, be appropriately clothed. Images of a pupil should not be published without the parent's or carer's written permission.

Pupils also need to be taught the reasons for caution in publishing personal information and images online.

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Pupils’ full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.
- Pupils work can only be published with their permission or the parents.
- Written consent will be kept by the academy where pupils’ images are used for publicity purposes, until the image is no longer in use.

How will staff be consulted?

- All staff must accept the terms of the ‘Responsible Internet Use’ and the ‘Staff Code of Conduct’ statement before using any Internet resource in the academy.
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet Policy, and Internet and E-mail Code of Practice and their importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff development in safe and responsible Internet use and on the academy Internet Policy will be provided as required.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such Smartphones, iPads, games players, are generally very familiar to children outside of the academy. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in the academy is allowed. Our academy chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The academy allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the academy allow a member of staff to contact a pupil or parent/ carer using their personal device.
- The academy is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the academy community is not allowed.
- Users bringing personal devices into the academy must ensure there is no inappropriate or illegal content on the device.

- Staff will use an academy phone when contact with pupils is required.
- Staff **should not** use personal mobile phones during designated teaching sessions, for any reason (texting, checking, phoning etc).
- Pupils are **strongly advised NOT** to bring personal mobile devices/phones to the academy. Any phones that are brought to the academy will be given to the class teacher who will store it securely and keep it there until the end of the day.
- The sending of abusive or inappropriate text messages outside of the academy is forbidden.

Academy Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any members of the academy community is not allowed
- Where the academy provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used
- Where the academy provides a laptop for staff, only this device may be used to conduct academy business outside of the academy.

Systems and Access

- You are responsible for all activity on academy systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC
- Do not allow any unauthorised person to use academy ICT facilities and services that have been provided to you
- Ensure you remove portable media from your computer when it is left unattended
- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time
- Do not introduce or propagate viruses
- It is imperative that you do not access, load, store, post or send from academy ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the academy or may bring the school or HCC into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the academy's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)

- Any information held on the academy systems, hardware or used in relation to academy business may be subject to The Freedom of Information Act
- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998
- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a written guarantee that they will irretrievably destroy the data by multiple over writing the data. Staff and Pupil Involvement in Policy Creation

Staff, governors and pupils have been involved in making/ reviewing the Policy for ICT Acceptable Use Review Procedure

- There will be on-going opportunities for staff to discuss with the Online-Safety coordinator any Online-Safety issue that concerns them
- There will be on-going opportunities for staff to discuss with the SIRO/AIO any issue of data security that concerns them
- This policy will be reviewed every (12) months and consideration given to the implications for future whole school development planning
- The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way

Online skills development for staff:

- ✓ Our staff receive regular information and training on online issues through the co-ordinator at staff meetings.
- ✓ All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of online and know what to do in the event of misuse of technology by any member of the academy community.
- ✓ All staff are aware of how to report and incident and have been introduced to the incident log.
- ✓ All staff have agreed to and signed the academy's Acceptable Use Agreement.
- ✓ New staff receive information on the academy's Acceptable Use Agreement as part of their induction.
- ✓ All staff are encouraged to incorporate online activities and awareness within their lessons. A progressive curriculum for online safety is ongoing and implemented across the academy.

Online information for parents/carers:

- ✓ Parents/carers are asked to read through and sign the Acceptable Use Agreement alongside their child. Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the academy website.
  - ✓ The academy website contains useful information and links to sites like Thinkuknow, Childline, CEOP and the CBBC Web Stay safe page.
  - ✓ The academy will send out relevant online information through newsletters and parents meetings (ie: Digital Parenting magazine).
  - ✓ Parents are invited to an online workshop during the year to keep them updated and give out advice.

Photographs taken by parents/carers for personal use:

On the event of parents/carers wanting to take photographs for their own personal use, the academy will demonstrate our protective ethos by announcing that photographs taken are for private retention and not for publication in any manner, including use on personal websites, e.g. academy performances and assemblies etc. Parents/ carers will be asked to sign a form agreeing to this alongside AUP's, or when their child starts our school or through home visits for new Early Years children and at the first visit for transferring students. As well as this, information will be provide on tickets and on the academy's website.

Social networking and personal publishing:

- The academy will block access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils and parents will be advised that the use of social network spaces outside the academy is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.
- Our pupils are asked to report any incidents of bullying to the school.
- School staff are advised **NOT** to add past or present children as 'friends' if they use these sites. (A child is anyone under the age of 18 years.)
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of the academy) will be raised with their parents/carers, particularly when concerning students' underage use of sites.

Writing and reviewing the online policy:

This policy - supported by the academy's Acceptable Use Agreement for staff, governors, visitors and pupils - is to protect the interests and safety of the whole school community. It is linked to the following mandatory academy policies including those for ICT, Home-school agreements, Behaviour, Health and Safety, Child Protection, and PSHE policies including Anti-bullying. Our online policy has been written by the academy, building on the DCC e–Safety Policy and government guidance including KCSIE, and has been agreed by the Senior Management Team and staff and approved by the Governing Body. The online policy and its implementation will be reviewed annually. As well as this, our school has formed a 'Digital Council' involving children from across the key stages.

Online bullying management:

- Online bullying (along with all other forms of bullying) of any member of the academy community will not be tolerated. Full details are set out in the academy's policy on anti-bullying and behaviour.
- There are clear procedures in place to support anyone in the academy community affected by online bullying.
- All incidents of online bullying reported to the academy will be recorded on CPOMs.
- There will be clear procedures in place to investigate incidents or allegations of online bullying.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence (children are encouraged to screenshot and show to a trusted adult).
- The academy 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.
- Pupils, staff and parents/carers will be required to work with the academy to support the approach to online bullying and the academy's online ethos.
- Sanctions for those involved in cyberbullying may include:
    - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
    - Internet access may be suspended at the academy for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the academy's Anti-bullying, Behaviour Policy or Acceptable Use Policy.
    - Parent/carers of pupils will be informed.
    - The Police will be contacted if a criminal offence is suspected.

Communications Policy

Introducing the online policy to pupils:

- Online rules will be displayed in all classrooms and discussed with the pupils at the start of each year. Specific lessons will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PSHE lessons/circle times/Anti-bullying week / E-Safety week

- An Online Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- An Online Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use.
- Pupils will be informed that network and Internet use will be monitored.
- The 'Hector the Protector' online button will be discussed and its use encouraged when inappropriate material is displayed.

Staff and the online policy:

- All staff will be given the School online policy and its importance explained.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is 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.
- Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- 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 pupils.
- All members of staff will be made aware that their online conduct out of 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.

Monitoring and review

This policy is implemented on a day-to-day basis by all school staff and is monitored by the online Coordinator.

This policy is the Governors‟ responsibility and they will review its effectiveness annually. They will do this during reviews conducted between the online Coordinator, ICT Coordinator, Designated Child Protection Coordinator, and Governor with responsibility for ICT and Governor with responsibility for Child Protection (online committee). Ongoing incidents will be reported to the full governing body.

The online policy will be revised by the online Coordinator.

The School online Coordinator is …F Brady……………………

Date implemented: September 2019 (this version)

Policy approved by Head Teacher: ……A Pybus-Coates……….. Date: September 2019

Policy approved by Governing Body: A. Coulthard (Chair of Governors) Date:

The date for the next policy review is September 2020.