DERBY HIGH SCHOOL
ESTABLISHED 1892

ICT POLICY AND PROCEDURES

This policy applies to EYFS as well as whole school

Owner	Senior network manager, SENDco, Deputy Head and Head of Primary
Authorised by	Head and Governors
Dated	September 2020
Review	September 2021

Related documents:

- Code of conduct for safe practice
- Safeguarding policy
- GDPR policy
- PSHE policy
- SENd policy
- Laptops policy
- Voice and voice recording apps policy
- Computing Rules and On-line Safety Agreement - Primary
- Computing Rules and On-line Safety Agreement - Seniors

Contents:

1. The role of ICT in school

- ICT is used by teachers and students to support learning and by administrative staff to provide effective and efficient school systems and procedures, e.g. finance, attendance and performance monitoring.
- ICT is used, wherever possible, to assist staff in their roles and responsibilities.
- Derby High School is committed to developing the use of ICT throughout the School organisation and to developing the skills and knowledge of students and staff.
- The Senior Network Manager, in conjunction with the Headteacher, Bursar, Head of ICT and Network Manager, will be responsible for all aspects of ICT administration and cross-school procurement.
- The school will endeavour to work with employees to ensure that they understand how to apply this guidance and enjoy the benefits of using ICT safely.

2. Aims of the policy

- To ensure robust systems for securing, monitoring and developing the use of ICT in school.
- To protect students, staff and parents safe from inappropriate content.
- To ensure staff, students and parents understand how to use digital technology appropriately and safely.
- To ensure GDPR compliance.
- To enable staff, pupils and parents to record events in the life of the school, where appropriate.
- To be clear about sanctions for misuse of technologies in school.

3. Managing the infrastructure

I. Funding:

- There is a central ICT budget for spending on consumables and capital items such as new or replacement hardware. This budget is controlled by the Senior Network Manager in regular consultation with the Headteacher. In addition, an ICT committee sits three times a year consisting of members of the senior leadership team, staff, a governor, the Network administrators and Head of ICT. A sub-group meets each half term to consider operational matters and to ensure cohesiveness between academic and technical ICT areas.

II. Hardware:

- There are a number of ICT facilities located around the school. There are specialist ICT suites in the senior and junior schools. The senior ICT suite is a bookable resource using an online system. Students are also encouraged to use these facilities outside normal lessons. The senior ICT suite has an open door policy before school and at lunchtimes. There are clusters of PCs in other areas

of the school such as the library and music department. A large number of classrooms have full audio visual facilities.

- The senior school has approximately 220 PCs and laptops. 18 classrooms have interactive whiteboards and most of the others have a standard data projector and screen. There are also a small number of Apple computers in the Design and Technology area of the school. Additional ICT hardware such as video and photographic equipment is bookable through the Network Manager.
- The school has 5 physical servers hosting around 20 virtual servers. Failover has been incorporated into the core network in all possible areas to ensure maximum up time.

III. Software

- The School's network is based on Microsoft Windows. Other main applications are the Schoolbase database application provided by Furlong Solutions and Microsoft Office 2016. There are numerous other subject specific applications.

IV. Managing access

- All of the students are encouraged to use the School's computer facilities whenever they need to support their learning. In addition, Years 12 and 13 have their own computer and printing facilities in the Sixth Form Centre.
- Students access shared learning resources for their subject from the shared folder area of the school network. This area has resources tagged by subject, topic, year group and teacher. It is also accessible from off-site locations using an internet connection.
- The school runs various software to allow staff, pupils and parents access to the school email system, their own work and the parent portal from outside school using the internet.
- A Bring Your Own Device (BYOD) network is provided for staff, Sixth Form students and guests.
- All users must accept a user-agreement before using any school ICT resource:
    - Key Stage 1 pupils: there will be an age appropriate level of explanation but pupils will not sign an agreement.
    - Key Stage 2 pupils: the rules will be explained and the pupils will be expected to sign the 'Primary Computing Rules and On-line Safety Agreement'.
    - Senior school pupils: the rules are explained and the pupils must sign the 'Secondary Computing Rules and On-line Safety Agreement'.
    - Parents/carers will be provided with a copy of the relevant agreement.
    - Staff must sign to say they accept the guidelines of this policy.
- The school maintains a record of all staff and pupils who are granted access to school ICT systems.

V. Security

- The Derby High School ICT system security is reviewed regularly.

- Virus protection is installed and updated regularly. If staff observe anything unusual after memory sticks, CDs, DVDs etc. have been brought into school, they should report it to the Senior Network Manager.
- All access and authorisations will be limited to nominated personnel. Different levels of access are established for different users (pupils, staff, senior staff etc) on the various systems operating in School.
- Staff and student accounts are password protected (see 'passwords')
- Encrypted memory sticks are available for staff, in line with data protection requirements.
- Users data is backed up locally twice daily. The schools system state data is backed up every weekend up to a disk which is moved to a fireproof safe in a different building during the week. These disks are on a 6 week rotation.
- Technical support is provided by 2 full time network support staff. Any staff member detecting any damage or malfunction should report it directly to the Senior Network Manager as soon as it has been detected.

VI. Data protection:

- Any personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations 2018.
- If a member of staff moves away from a computer logged into the system they must either logout or lock the computer.
- When projecting onto the board, staff must take care to ensure that sensitive material does not appear on the screen.

VII. Filtering and monitoring:

- In order to safeguard pupils, and in line with the PREVENT strategy, the school takes a robust approach to monitoring and filtering.
- It is prohibited to view, retrieve or download any content which the school would view as unsuitable, such as pornography or extremist material.
- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. If staff or pupils discover an unsuitable site, it must be reported to the Senior Network Manager.
- The school cannot accept liability for any inappropriate material accessed, or any consequences of internet access.
- We have robust web filtering built into Dell Sonicwall; this is based on a list of inappropriate websites which have been categorised by a third party. We can add websites to this list as we see fit.
- The filtering process looks for an blocks sites containing key words of concern e.g. Violence/ Hate/Racism/Illegal/Questionable Skills/Weapons

- The Network Manager monitors the log file of the sonic wall list of issues/blocks. This means that: a) any repeated searching by a particular student would be noted, reported to the DSL and followed up and b) if there was an unprecedented failure of the filter, this would be picked up very quickly by the change in length of blocked searches.
- Students are monitored at random during un-supervised use of computers by the Network Manager; any behaviour of concern is reported to the Designated Safeguarding Lead. We force the use of "safe search" on search engines to filter out the worst of the web.
- All teachers have access to Impero which allows them to view the screens of students in their lesson.
- Students are aware of Impero and know that we can see what they are doing – Impero is used in lessons to demo students work via the teachers machine, a small thumbnail of every monitor is on screen so if a student was doing something wrong the whole group would see it.
- If a student was identified as being at risk of being drawn into terrorism, their computer use would be closely monitored and access may be restricted.
- The BYOD network's internet access is filtered as stringently as any other computer on the network
- The school will audit ICT use regularly, to establish if current on-line safety procedures are appropriate and effective.

VIII. Software and Licensing

- Software used on School ICT resources must be solely that which has an accompanying individual or site license. The Senior Network Manager is responsible for maintaining records of this.
- Any software that is purchased should be passed to the Senior Network Manager for installation. The Senior Network manager will keep original copies of software and site licenses.
- Internet-derived materials and video recorded must comply with the relevant copyright and licensing laws.
- The Senior Network Manager keeps an inventory of hardware and software used in School.
- The school will ensure the monitoring of software and that appropriate procedures are in place to highlight when action needs to be taken by the school.

IX. Passwords

- Users must ensure their passwords are secure: they should not be obvious, for example a family name or birthdays.
- Users should not allow anyone else access to their password: passwords must be changed if a member of staff believes that there is a possible security breach.
- Passwords should be a minimum of 8 characters and should be alphanumeric.
- Users are advised to change their passwords regularly.
- These guidelines apply especially to staff, who have access to sensitive student data.
- Staff are advised to use different passwords for schoolbase and the school network. (This is essential for SLT members.)

X. Training

- New staff are given training on the school systems when they first join the school.
- Training on any new software or programs is given either during INSET days or voluntary drop in lunchtime sessions as needs dictate.

XI. Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

4. Guidelines re the use of technology in school

- In addition to guidelines provided by this policy, staff must adhere to the Code of Conduct for Safe Practice, the Safeguarding policy and specific guidance given in policies such as the laptops and dictaphone policies.
- The priority for the use of IT equipment should always be given to staff who are using it for a purpose directly related to their teaching or school responsibilities, eg. for organising school trips, producing documents/worksheets/reports and lesson planning.
- Staff should not use the computers for personal email, games or personal arrangements (e.g. booking private train tickets) during any of their lessons. At other times, use of computers for personal reasons is acceptable to School, as long as it is not done to excess and does not stop other members of staff from using computers for teaching related work.

(a) Use of email

- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- Any suspicious emails should be reported (not forwarded) to the network manager. On no account should attachments accompanying such messages be opened. If in any doubt about the validity of an e-mail, users must consult the relevant IT staff for advice.
- The forwarding of chain letters is not permitted.

Additional guidelines for pupils:

- Pupils must report any instance of abuse or misuse of the email to their form tutor or Head of Key Stage in the first instance. This includes any instance of offensive or inappropriate e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone, without specific permission.

Additional guidelines for staff:

- Staff should use only their Derby High School email accounts to communicate with each other, pupils or parents for school business.
- Pupils' full names should not be used in the email subject header. The word 'confidential' should be used in the message header and the name only referred to within the message content.
- It is acknowledged that occasionally staff may need to use their school email account to send a personal message; staff must exercise caution when doing this.

(b) Use of phones and cameras (increasingly a single device)

'Photography' includes photographic prints, streaming media, video, film and digital imaging, created using any device including, but not limited to cameras, video cameras, phones, tablets, etc.

Our rules are based on respect and consideration for others, and the desire to minimize disruption in lessons and around school.

Guidelines for Junior school pupils

- If a camera or phone is brought to school for any reason it must be given to the form tutor first thing for safekeeping during the day and collected at home time.

Guidelines for Senior school pupils

Any pupil taking a picture/video of other pupils should have their verbal permission and it is expected that these pupils will generally fall into the same friendship grouping or other common grouping (eg form, house, activity group).

- Any pupil taking a picture/video to include a member of staff must have the permission of the member of staff.
- Photographs taken in school must not be displayed publicly or via the computer or any Social Networking Internet Sites such as Facebook, myspace, Snapchat or Bebo without the written permission of the Head.
- The above conditions apply to video clips taken on any device.
- Members of the Sixth Form are exempt from the following guidelines, but must use their phones only within the Sixth Form Area, keeping them switched off in their bag during lessons. If this agreement is broken, including being seen with the phone elsewhere in the school, the Head of Sixth Form will be notified.
- Mobile phones belonging to U3-U5 pupils may be brought into school and should be properly named.
- Mobile phones must not be used by U3-U5 pupils between 8.30am and 3.35pm or 4.00pm (depending on the length of the school day) except in an authorised emergency or when directed to by a class teacher during a lesson.
- Mobile phones belonging to U3-U5 pupils must be kept in lockers, switched off. They should not be kept in bags or pockets.
- If U3-U5girls are attending P.E. matches, the P.E. department will look after them but cannot take ultimate responsibility for the safety of the phones.
- For school trips, it is at the discretion of individual members of staff as to the arrangements for the use of mobile phones.
- School is not responsible if a mobile phone is lost or stolen.
- Any U3-U5 pupil in possession of/using a mobile phone in school time will have it confiscated for the remainder of the day. 3 penalty points will be issued which will result in an automatic school detention and parents will be informed. If this happens twice in one term the phone will be confiscated and will only be returned to a parent. Pupils are advised that no exceptions will be made.

- Confiscated pupil phones will be handed to the Head of Key Stage or Deputy Head. Penalty points will be recorded by the teacher who observed the incident.
- If a pupil needs to contact parents during the day she should ask at reception.

Guidelines for staff:

- Staff must think carefully about whether or not it is appropriate to communicate with a pupil via their mobiles. Staff must take care to ensure that any contact via mobile phones or the internet cannot be misinterpreted by the pupil or in a way that would lead a reasonable person to question their actions.
- Some communication is an accepted part of school life, especially as the pupils get older. E.g. phoning captains of sports teams, using staff numbers as contacts for Duke of Edinburgh Award etc.
- If a member of staff needs to use their personal mobile but wishes to protect their number they should enter 141 before the number they are dialing. Pupil numbers held by staff for expeditions or trips must be deleted at the end of the trip. Ideally, staff should take the school phone on trips and use that contact number only.
- Staff must consider safeguarding regulations when taking photographs and consult the list of students whose parents have not given permission for their photograph to be used.
- Staff may take photographs of their class, for display work, to record achievement and for a record of events. Staff can only take these images for use in school.
- Staff are advised not to use their own mobile phones to take photographs of pupils for their own protection. If it is an occasion when staff have no alternative but to use their own device(e.g. phone/ipad) to take pictures or video of pupils - e.g. whilst on a school or fieldwork trip - the photos/video must only be for use in school. They must be downloaded onto the school network within a reasonable time frame.
- Any photographs taken on personal devices must be uploaded to the school network as soon as possible and the picture deleted from the personal device.

Published content and the school website:

- The Marketing Manager will have overall editorial responsibility for the website and will ensure that published content is accurate and appropriate.
- Written permission, using the approved permission form from parents or carers, will be obtained before photographs of pupils are published on the school website.
- Pupils' full names will not be used anywhere online, other than the password-protected areas on the school website, particularly in association with photographs.
- Photographs that include pupils will be selected carefully so that images of individual pupils cannot be misused, as far as it is possible to do so.
- Staff or pupil personal contact information will not generally be published.
- Any contact details given online will direct communications to the school office.

Guidelines for parents:

Parents are usually permitted to use personal photography/video equipment to record events in which their children take part.

- Parents are expected to be considerate when taking photographs and video, so that the children participating in the event and other parents are not inconvenienced or disturbed during concerts, performances or other events.
- Parents using camera equipment should ensure that the focus of their photography is on their own children.
- For the safety of our students and to comply with data protection regulations, parents are asked not to post photographs which feature children other than their own on any public area of the internet or via social media
- The Head reserves the right to withhold permission for photography at any event.

NB A reminder of points 1-4 will be given at the start of plays/concerts.

(c) Video-conferencing

- Video-conferencing will be set up with the advice of the Senior Network Manager with known organisations to ensure quality of service and appropriate security.
- Pupils should ask permission from the supervising teacher before making or answering a video-conference call.
- Video-conferencing will be appropriately supervised for the pupils' ages.

(d) DVD and film use

The showing of DVDs and video to students is regulated by copyright laws.
http://era.org.uk/the-licence

- Our ERA Licence allows us to record, in whole or part, films and programmes owned or represented by ERA members **for non-commercial, educational use** (see **http://www.era.org.uk/** for current list).
- The licence includes all scheduled free-to-air radio and television broadcasts, plus content from online and on-demand services, including podcasts, where permitted by the service. Users should check the terms and conditions of the services for details. Non-scheduled internet transmissions (e.g. YouTube) are not broadcasts and are therefore not covered by the ERA Licence.
- Programme content must be used as it has been broadcast, and not edited; original extracts or clips may be selected. Programme credits should not be edited from recordings. Provisions within The Copyright and Rights in Performances (Disability) Regulations 2014 may support educational establishments making accessible copies for the personal use of a disabled person in certain circumstances (e.g. when subtitles or audio description is required). Please check appropriate regulations before doing so.
- Film and film clips recorded for such educational use may be stored in analogue or digital format. Digital recordings may only be stored and shown via secure networks operated by or for the school.
- **All recordings,** whether analogue or digital, must be **clearly labelled with the date, name of broadcaster, programme title and the following specific wording: 'This recording is to be used**

only for educational and non-commercial purposes under the terms of the ERA Licence'. There are ready made labels available in the grey trays in the staffroom. Failure to label recordings may lead to licences being withdrawn.

- Storage of programmes under ERA licence: programmes recorded **after 30th May 1990** under the terms of an ERA Licence can be **retained indefinitely** by a licensed educational establishment whilst it continues to hold a valid ERA Licence. Programmes recorded prior to 1st August 1989 are governed by the terms of the licence under which they were recorded. Most licences did not permit the indefinite retention of recordings. Recordings which are no longer needed or covered by a current Licence must be destroyed and may not be sold or otherwise dealt with.

  Providing these terms are adhered to, no further record need be kept of when films or clips are shown under the ERA licence.
- Showing any film for purposes other than education, films which have been purchased as DVDs rather than recorded, or which have been produced by non-ERA members must be covered by either PVSL or MPLC licence. [Broadly speaking, PVSL covers the main Hollywood studios (http://www.filmbank.co.uk/content.asp?id=45178 for current list) and MPLC represents independent film studios.] This applies, **whether or not a charge is made for viewing**. This would include Movies and Munchies, any fundraising events, assemblies and any extra-curricular, after-school or end of term activities. PVSL require us to submit a quarterly licence return, though ERA and MPLC do not. Therefore, for ALL **films** (not television programmes) shown in school, please complete a PVSL licence return and pass to the bursar's assistant. PVS will disregard films covered by other licences. This process will ensure that we are complying with the PVS licence terms, without having to check which licence applies for each film we show.

Procedures for showing DVDs/videos in class:

- Staff members must have recently watched the entirety of the film or extract being shown to students, watching with their intended audience in mind. No DVD/video that the member of staff has not watched in its entirety should be shown to pupils.
- No DVD/video with an age classification may be shown in full to any pupil under the age of the classification – except in the following situations:
  - Please be careful where individual pupils are out of age group. If permission is required for an individual case please refer this to the Deputy Head: parental permission will need to be sought.
  - A request to show a film in full for educational reasons to a class under the age of classification must be made to the Deputy Head (sufficient time allowance must be given for the decision to be taken). If the individual case is deemed reasonable then permission slips must be obtained from the parents of the girls under the classification age. Each new film that is to be shown in this way must be raised as an individual case. Repeats of a previously agreed request (for the same film to the same age group for the same reason) should be notified to the Deputy Head: but agreement is taken as given and permission slips can be sent out without further confirmation. Please remember that as student

cohorts vary in their maturity and ability, films shown out of classification must be re-watched by the teacher each year and a fresh decision made about suitability for the individual cohort must be made each time.

- A short extract may be shown from a DVD/video with an age classification to pupils below that age if the teacher judges the extract is suitable for that age group. The teacher must have watched the extract in full previously and made a judgement with that particular group in mind. (As above, student cohorts vary in their maturity and ability, so extracts shown out of classification must be re-watched by the teacher each year and a fresh decision made about suitability for the individual cohort must be made each time. Notification must be made to the Deputy Head in advance of screening.)

(e) Use of social media

Guidelines for staff

- Staff should assume that anything they write (regardless of their privacy settings) could become public so should ensure that they are professional, maintaining a clear distinction between their personal and professional lives.
- Any use of social media made in a professional capacity must not:
    - Bring the school into disrepute;
    - Breach confidentiality
    - Breach copyrights of any kind.
    - Bully, harass or be discriminatory in any way.
    - Be defamatory or derogatory.
    - Breach data protection regulations.
- The school appreciates that staff may make use of social media in a personal capacity. However, staff must be aware that if they are recognised from their profile as being associated with the school, opinions they express could be considered to reflect the school's opinions and so could damage the reputation of the school. For this reason, staff should avoid mentioning the school by name, or any member of staff by name or position. Opinions should follow the guidelines above so as not to bring the school into disrepute, breach confidentiality or copyright, or bully, harass or discriminate in any way.
- Staff must be aware of the security settings they use on social networking sites to ensure potentially embarrassing material cannot be accessed by pupils, parents or the general public.
- Social media may be used to interact with students, only for educational rather than social reasons. For example, e.g. setting up a subject page for support with homework is acceptable but individual messages to students' profile pages is not.
- Staff must not allow pupils to access their personal pages on social networking sites nor accept as friends any current pupils or any former pupils under the age of 21 (since many former pupils remain in contact with pupils in lower years or have younger siblings still in the school). Staff should not accept or seek such connections because this could potentially be construed as 'grooming'.
- An exception to this rule may be made where the current or former pupil is a relative or close family friend of the member of staff. In this situation, it is the responsibility of the member of staff: to notify the Head of the situation in writing; to ensure that their own security settings do not allow the young person access to any potentially embarrassing material; to ensure their other contacts are aware of the connection if any material they post can be seen by the current/ex-student.
- A member of staff wishing to make contact with a former pupil should consider carefully the nature and reason for this communication and, where it is appropriate, do so via their school e-mail, not through a social networking site.

Guidelines for pupils

- Pupils will be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future.
- Pupils will be advised on security settings and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications.
- Pupils will be encouraged only to invite known friends and deny access to others.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

Please also see the safeguarding policy

5. The ICT curriculum for students

Educating students about the use of ICT is both a discrete element of the school curriculum and included within other curriculum areas as appropriate.

- Clear boundaries will be set and discussed with staff and pupils, for the appropriate and safe use of the internet and digital communications.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

In years U3, L4 and U4 the students receive one double ICT lesson per week. In year L5 students receive one double a fortnight. In year U5 students then again have one double lesson a week of ICT

Key stage 3 – ICT and Computing

Year U3: Students are introduced to the school ICT system and some of the programs on the senior school network that they might find useful in the future. They learn about e-mail and online safety as well as being introduced to spreadsheets and desktop publishing. Students also get an opportunity to improve their typing speed and start to learn touch typing.

Year L4: Students change from being a program user to being a program designer by creating a game using simple programming. They also get an opportunity to learn animation and how to use and create QR codes. In this year students build on their knowledge of spreadsheets and also completed another online safety module.

Year U4: In this year, students are introduced to more complex 3D and 2D design programs that they may use elsewhere in the school. They will also create their own website using specialty software and learn how to embed multimedia elements into their site. Students also have the opportunity to create database forms and tables and to construct queries to interrogate their database.

Key stage 4 ICT

Year L5: Students start the year by reviewing key skills that will be needed for their GCSE such as use of spreadsheets and advanced techniques in Word and PowerPoint. Students are introduced to the world of artificial intelligence, they then use functions and methods to code an AI bot in the lesson. Students also learn to code Karel the dog and are introduced programming in HTML and Javascript.

Year U5: Students have the opportunity to investigate uses of 3D printers in the workplace and in the future. They also learn practical skills using a 3D design program and convert to file formats that will print their designs in 3D. They then move on to used advanced PowerPoint and Powtoon to fine hone their presentation skills which will be useful in the future. They also complete a project looking at the use of ICT through different stages of their future lives, for example looking at tax, mortgages, applying through ucas and searching for jobs.

6. The use of technology to support students with learning difficulties and disabilities (LDD)

The school is committed to using ICT where possible to support students with LDD. Smart board mind mapping, software to allow computer screen colour changes and online touch typing tutorials are examples where ICT is used in school for this purpose.

The senior network manager liaises with the SEND co-ordinator about specific ICT support for individual girls.

a) Laptops for use in lessons and exams

Please see the **Laptop policy** for guidance.

b) Use of dictaphones

The school will sometimes allow parts of an academic lesson to be recorded using a Dictaphone or similar recording device.

Please see the Dictaphone policy for guidance.

7. E-safety

Please also refer to the safeguarding policy

E-safety is supported by all aspects of this policy:

- Maintaining a secure infrastructure with robust filtering processes.
- Guidelines for students, staff and parents about safe practice in all aspects of ICT use.
- Advising all users that their use of the school network and the internet can be monitored and traced to an individual user (from PCs, laptops and personal devices).
- Training for new staff.
- The related requirement for students across the school to agree to their age-appropriate Computing Rules and Online-Safety Guide
- On-line Safety rules displayed in all rooms where computers are used by pupils, appropriate to their age.
- The ICT and PSHE curriculum for pupils, reinforced through assemblies and across the curriculum to maintain awareness.
- Supervision, by SLT, of staff that manage filtering systems or monitor ICT use, working to clear procedures for reporting issues.
- Raising parents' awareness through school literature, the school website and via relevant, targeted contact whenever relevant.

8. Sanctions for misuse

- In the event of unsafe and/or unacceptable behaviour, disciplinary or legal action (including gross misconduct leading to dismissal) will be taken, if necessary, in order to support safer working practice and minimise the risk of malicious allegations against staff and others who have contact with pupils.
- Complaints of internet misuse will be reported to the Designated Safeguarding Lead in school and the Senior Network Manager.

- Any staff misuse that suggests a crime has been committed, a child has been harmed or that a member of staff is unsuitable to work with children will be reported to the LADO within one working day.
- Any complaint about staff misuse must be referred to the Headteacher and, if the misuse is by the Headteacher, it must be referred to the Chair of Governors.
- Pupils, parents and staff will be informed of the complaints procedure.
- Each case of misuse of technologies by a pupil will be considered separately and appropriate sanctions put in place. Permanent exclusion for the most serious cases, such as persistent bullying of another pupil, may result.

APPENDIX A: Annual on-line safety audit document: Completed February 2019

Has the school an e-safety safety policy that is regularly reviewed?	Yes
The policy is available for staff at:	S:\Whole School\Staff Handbook\Policy Documents
The policy is available for parents/carers at:	Yes: on the school website
The member of the Senior Leadership Team is:	Mrs Claire Bellman - Designated Safeguarding Lead (Seniors) Mrs Rachel Youngman -(DSL Primary)
The responsible member of the governing Body is:	
The Senior Network Manager is:	Mr William Bentley
The e-safety co-ordinator is:	Mr S Williams – Head of ICT - Primary
Have on-line safety materials from CEOP and Becta been obtained ?	Yes
Has on-line safety training been provided for a) pupils and b) staff?	a) Yes: SWi, SHi and b) Yes: ICT policy and procedures
Do all staff sign a Code of Conduct for ICT at start of employment?	Yes ICT policy and procedures
Are all pupils aware of the School's on-line safety rules?	Yes (SWi, CHo)
Are on-line safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	Yes (SWi, CHo)
Do pupils sign an agreement that they will comply with the School's on-line safety rules?	Yes AMa, SWi,
Are parents provided with information about this agreement?	Yes AMa,
Is there a clear procedure for a response to an incident of concern?	Yes: Usual procedures for pastoral/disciplinary incidents to be used. AJO/JHa to direct Network manager to investigate actions on school system if necessary. Action taken to remedy any security issue as soon as possible and interim safeguards put in place.
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	Yes

Is personal data collected, stored and used according to the principles of the Data Protection Act?	Yes: database does – confirmed by Schoolbase Yes: DHS complies with Data Protection regulations
Has the school-level filtering for internet access been designed to reflect educational and safeguarding objectives and approved by Headteacher/SLT?	Yes (WBe)
This audit has been completed by:	ACh, WBe
Other contributors include:	SWi CHo AMa MMi

Appendix B: Staff code of conduct for ICT use

I confirm that I have read and accept the guidelines contained within the ICT policy and procedures.

Signed……

Dated…….