ICT POLICY AND PROCEDURES

This policy applies to EYFS as well as whole school

Owner	Senior Network Manager, SENDCo, DSL, Head of Primary
Authorised by	Head and Governors
Dated	Autumn i, 2023
Review	Autumn i, 2024

Related documents:

- Code of Conduct for Safe Practice
- Safeguarding, CP and CME policy
- GDPR policy
- PSHE policy
- SENd policy, inc. word processor and voice recorder procedures
- Computing Rules and On-line Safety Agreement - Primary
- Code of conduct for ICT use – Seniors
- Code of conduct for live online communication
- Acceptable use agreements for staff and pupils.
- Primary computing policy

Contents:

1. The role of ICT in school

- ICT is used by teachers and pupils 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 pupils 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 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 pupils, staff and parents safe from inappropriate content.
- To ensure staff, pupils 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 Bursar in regular consultation with the Headteacher.

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. There are clusters of PCs in other areas of the school such as the library and music department. All classrooms have full audio visual facilities.
- The senior school has approximately 220 PCs and laptops. 33 classrooms have interactive whiteboards and most of the others have a standard data projector and screen. There are three banks of laptops – one in DT, one in Physics and one in the library. Additional ICT hardware such as video and photographic equipment is bookable through the Network Manager.

- The Primary School ICT suite contains 21 machines and is the location for timetabled Computing lessons. It is also a bookable resource at other times. There are teacher machines in each classroom, 2 in each staff room and 21 in each of the infant and junior halls.
- The school has 4 physical servers hosting around 20 virtual servers. Failover has been incorporated into the core network as far as is reasonable to ensure maximum up time.

III. Software

- The School's network is based on Microsoft Windows. Other main applications are the ISAMs database application and Microsoft Office. There are numerous other subject-specific applications.

IV. Managing access

- All of the pupils 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.
- Pupils 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. The school runs Microsoft 365 to allow staff and pupils access to the school system, The ISAMs parent portal is also available from outside school using the internet.
- A segregated Bring Your Own Device (BYOD) network is provided for staff, KS5 pupils 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 and pupils sign the 'Primary Online Safety Agreement' .
    - Key Stage 2 pupils: the rules will be explained and the pupils will be expected to sign the 'Primary Online 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 on appointment (see appendix B).
- 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. Staff should report to the Senior Network Manager anything unusual that they observe, following digital materials or devices being brought into school and connected to the school infrastructure.

- 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 pupil accounts are password protected (see 'passwords') Two-factor authentication is enforced for staff logging on to Office 365 systems and iSAMS
- User and system state data is backed up using hardware which is housed in a different building to the main servers. These backups are further saved to the cloud using VEEAM.
- Technical support is provided by 2 full time network support staff. Any staff member detecting any damage or malfunction should report it via the Helpdesk facility, immediately upon detection.
- The use of USB memory devices is, in general, disabled except in circumstances where no alternative is available – for example accessing memory cards in the Art department. If, in exceptional circumstances, a stick is used, it will be scanned before use by the IT support team and the relevant PC will have ports enabled temporarily.

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 or pupil 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. We advise staff to use extend mode when projecting to prevent this from happening.
- Staff understand their duties involving GDPR and have received advice in proper use of data in a remote working environment

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. The Designated Safeguarding Lead is responsible for ensuring that filtering and monitoring requirements are in place, and that the systems are monitored, reviewed and audited regularly, and should a need arise.
- It is prohibited to view, retrieve, download or distribute 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. The DSL and Network Manager will meet to review parameters currently in place, to risk assess current settings and configurations and their impact on teaching and learning. It is necessary to be careful to balance risk to pupils and the impact on teaching and learning, putting reasonable restrictions in place at all times. It is also worth remembering that sdue 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 Network Management Team. The school cannot accept liability for any inappropriate material accessed, or any consequences of internet access.

- The filtering process looks for and blocks sites containing key words of concern e.g. violence/ hate/racism/illegal/questionable skills/weapons. The effectiveness of this is tested across all school devices on a regular basis by the DSL and Network Manager. A new concern can also trigger further investigations into the systems and procedures in place.
- Internet access is overseen by the Network Management Team.
- We use two different systems in order to ensure a robust filtering and monitoring system.
- We subscribe to Smoothwall filtering to filter and block unsuitable websites in the school. This is based on a list of inappropriate websites which have been categorised by a third party and which is updated regularly. We can also add websites to this list as we see fit. The DSL receive a daily email of sites that have been blocked for individual users and this is followed up as appropriate.
- We also subscribe to Smoothwall monitor. This system alerts the DSL team whenever a pupil searches for or types in concerning content. This is via email or telephone, should the need be urgent. Any alerts are checked in a timely manner and followed up where necessary.
- We also subscribe to a secondary system, Impero, which is actively used to monitor usage in person by the teacher in the lesson with the pupils. This system captures screenshots of any inappropriate or concerning use of the IT systems. This will also send an email alert to the DSL team and Network Manager. This programme also allows teachers to see the screens of all students in the lesson, send messages, project screens and freeze screens. It also allows the DSL to run a report of captures for individual dates, users or PCs.
- Staff are instructed touse Impero to monitor usage whenever they are using school computers with pupils during their safeguarding induction, and regularly reminded. Staff should follow up any concerns raised as appropriate, either using the Behaviour Policy, or by raising a concern with the DSL team.
- Pupils are aware of both Smoothwall and Impero and know that we can monitor what they are doing.
- Pupils 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.
- If a pupil 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. Pupils are required to sing in using their school credentials, as they would on a PC on site.
- The school will audit ICT use regularly, to establish if current online safety procedures are appropriate and effective.
- We are not able to filter and monitor devices in school but not on our system, e.g. phones on a mobile network. We are aware of the risk of this, hence any junior students who is allowed a mobile device due to taking the school bus, is instructed to leave the device with the junior

receptionist on entry to school and are not allowed phones on site, senior students must store phones in lockers during the school day (please see Senior School Information booklet for further guidance). Sixth formers are allowed them in the sixth form centre only. This approach is constantly under review and is strictly enforced by staff. We also write to parents at the start of each academic year to make sure that they are also aware of this.

- Phones may be allowed on trips for senior pupils, subject to the student code of conduct and the ICT Code of Conduct. All students sign both codes. Trip Leaders have the right to refuse phones on trips, and to ask for phones from students should the code of conduct be broken.

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.
- There is 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 must 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 must contain 3 of the following features:-
    - Uppercase letters (A,B,C)
    - Lower case letters (a,b,c)
    - Number (1,2,3)
    - Symbol (!,",£)
- In line with current guidelines, staff and pupils are not forced to change their passwords regularly (Link - NCSC Guidance)

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.
- An obvious example of this is the use of AI in schools, both by staff and students. We are evaluating the benefits and dangers of this emerging technology as it develops and will craft a school approach in time.

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 the SENd policy, for example, protocols surrounding laptops and assistive technology.
- 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.
- Personal banking is not permitted on the school network, including BYOD.

(a) Microsoft Teams

See student ICT code of conduct for detailsStudents are reminded that Teams is a school programme and therefore should be used for learning purposes only. Any communications should be executed in a formal manner.Student chat disabled for primary students. Senior students are able to chat with teachers, but cannot create new groups or start video calls with other students.

(b) 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 phishing tool.. 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.
- When forwarding an email, great care should be taken not to forward anything inappropriate or confidential.
- Always use isams to double check email addresses and home situations before emailing.

Additional guidelines for pupils:

- Pupils must report any instance of abuse or misuse of the email to their class teacher, form tutor or Head of Year 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, parents or 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.

(c) Use of phones and cameras

'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 EYFS

- As part of their development, EYFS children will have access to a broad range of IT resources but are not allowed to bring mobile phones or devices into school.

Guidelines for Junior and Senior pupils

- If a device is brought to school by a junior school pupil, it must be given to primary reception for safekeeping during the day and collected at home time.
- Senior school pupils may bring mobile phones into school, subject to the regulations in the Senior School Information Handbook. Cameras or video-cameras may not be brought into school or used without explicit permission from the Head, Senior Deputy Head or Deputy Head (pastoral).
- 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 network without the written permission of the Head.
- The above conditions apply to any image or audio recording taken on any device.
- All personal property brought into school should be named, so it can be returned if misplaced.
- School is not responsible if a mobile phone or other device is lost or stolen.
- If a pupil needs to contact parents during the day may do so from reception.
- Senior school pupils sign an ICT Code of Conduct and agree to abide by the conditions therein, on school site and on school trips.

- Guidelines for staff are contained with the Code of Conduct for Safe Practice and must be read and adhered to

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 be published.
- Any contact details given online will direct communications to the school office.

Guidelines for parents:

- Parents, carers and visitors are reminded that, due to photo and video consent permissions, they cannot take pictures and videos of children during a performance.
- The school will make every attempt to record performances and capture photographic images, which will be shared with families, as appropriate, to ensure photo and video consent permissions are adhered to.
- We will also attempt to provide opportunities, where appropriate, for photographs of your own children.
- Parents should not otherwise take photographs of any children on the school site without express permission of the Head. This is to safeguard the children.
- Within the parameters outlined above:
    - 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 pupils and to comply with GDPR, 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. The following notice will be read/included in the programme for public events:

Privacy and safeguarding notice:
Please do not take video of any of the performance. We would also prefer you not to take photographs until afterwards, when performers can give consent to being photographed, and to avoid distracting both the cast and other members of the audience. Any photographs taken of children other than your own must not be shared on social media.

(d) 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.

(e) DVD and film use

The showing of DVDs and video to pupils 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 pupils, 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 pupils 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 pupil 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, pupil 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.)

(f) Use of social media

Guidelines for staff are contained with the Code of Conduct for Safe Practice and must be read and adhered to.

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 pupils

Please see the Primary Computing Policy for details of the primary curriculum

Senior curriculum:

Educating pupils 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.
- All pupils in Key Stage 3 complete a project on online safety including, but not limited to, online bullying, digital footprint, trolling, social media training and safety regarding sharing photos, online gambling, gaming disorder and online grooming.

In years 7-9 the pupils receive one double ICT lesson per week. We also use external providers for workshops and talks around the dangers of social media and other online safety topics.

Key stage 3 – ICT and Computing

Year 7: Pupils 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. Pupils also get an opportunity to improve their typing speed and start to learn touch typing. Pupils do programming in Scratch.

Year 8: Pupils 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.. In this year, pupils build on their knowledge of spreadsheets and also completed another online safety module

Year 9: In this year, pupils 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. Pupils also have the opportunity to create database forms and tables and to construct queries to interrogate their database.

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

The school is committed to using ICT where possible to support pupils 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 pupils.

a) Laptops for use in lessons and exams

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

b) Use of assistive technology

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

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

Online SafetyPlease also refer to the **safeguarding policy**

Online Safety is supported by all aspects of this policy:

- Maintaining a secure infrastructure with robust filtering processes.
- Guidelines for pupils, 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.
- External input from online safety professionals
- The related requirement for pupils across the school to agree to their age-appropriate Computing Rules and Online-Safety Guide
- Online 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, face to face events and via relevant, targeted contact whenever relevant. Consequences of 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 consequences 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 November 2023

Has the school an e-safety safety policy that is regularly reviewed?	Built into the SG policy and Code of Conduct for staff and students.
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 (whole school)
The responsible member of the governing Body is:	Mrs N Read
The Senior Network Manager is:	Mr Martin Lindau
The e-safety co-ordinator is:	Mr S Williams – Head of ICT Ms Danielle Hyland - Primary ICT lead
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 – ICT lessons, PSHE and Status Social workshops b) ICT policy and procedures, training events (October /November 2021 all teaching staff completed training) Online safety training is also provided for parents - new parent induction, supporting your child through the exam years and in weekly highnotes
Do all staff sign a Code of Conduct for ICT at start of employment?	Yes
Are all pupils aware of the School's on-line safety rules?	Yes (SWi, DHy)
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, DHy)
Do pupils sign an agreement that they will comply with the School's online safety rules?	Yes CBe
Are parents provided with information about this agreement?	Yes CBe
Is there a clear procedure for a response to an incident of concern?	Yes: Usual procedures for pastoral/disciplinary incidents to be used. Head/Deputy Head or Head of Primary (as relevant) 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: ISAMs 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 (CBe, MLi)
This audit has been completed by:	CBe MLi
Other contributors include:	SWi DHy

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;
- Code of Conduct for Safe Practice;
- Safeguarding, CP and CME policy;
- SENd policy on the use of laptops and assistive technology.

Signed……

Dated…….