E-Safety Policy

St Agnes C of E Primary School

Approved by:	Mr Chris Cartwright
Last reviewed on:	September 2022
Next review due by:	September 2023

E-Safety Policy

Mission Statement

'Learning together in God's Love'

We are an inclusive Christian family, who ***'Learn Together In God's Love'*** with mutual respect, tolerance and kindness. ***We treat each other as we would like to be treated (Matthew 7v12)*** this allows us to thrive in our education, friendships and journey through life. We are proud to say we are all equal.

Through the range of experiences we off to all our pupils we encourage an understanding of the meaning and importance of faith and promote all the Christian Values. We particularly focus on Responsibility, Creativity, Forgiveness, Perseverance, Hope, Thankfulness and Friendship. These Christian values form the basis of our vision and are embedded throughout out school life and underpin all our teaching.

St Agnes is a small school that supports our community by providing an education of the highest quality within the context of Christian belief and practice. We work closely with our families to ensure they are fully supported and cared for

We expect everyone at St Agnes C of E Voluntary Aided Primary School to follow 'The Great Expectations' –

Be Safe
Be in the right place at the right time
Do your best
Handle your emotions
Use appropriate language
Cooperate
Respect everyone and everything

1. Introduction

1.1. This document is a statement of the aims and effective approaches to e-safety at St Agnes C of E Voluntary Aided Primary School. Safeguarding children, including e-safety is everyone`s responsibility.

2. School E-Safety Policy

2.1. The headteacher takes responsibility for all child protection policies and guidance in the school. The headteacher is the designated person for child protection and therefore the E-Safety Co-ordinator. This role will also overlap with the deputy designated person for child protection, the Computing Co-ordinator, and the schools ICT Technicians. They will work collaboratively to ensure ever-changing issues relating to the Internet and its safe use. The policy will be reviewed regularly. Changes will be made immediately if technological or other developments so require.

3. What is E-Safety?

3.1. It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school approach to online safety empowers our

school to protect and educate pupils and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

3.2. The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

3.2.1. **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

3.2.2. **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.

3.2.3. **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images(e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

3.2.4. **Commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

3.3. Considering the 4Cs (above) will provide the basis of an effective e-safety planning.

4. Aims & Objectives

4.1. Our school will ensure online safety is a running and interrelated theme whilst devising and implementing policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead and any parental engagement.

5. Responsibilities of the E-Safety Co-ordinator

5.1. The responsibilities of the E-Safety Co-ordinator include :

5.1.1. Updating the E-Safety, Computing and Acceptable Useage policies;

5.1.2. Consider the 4Cs (above) as the basis of an effective online policy.

5.1.3. Ensuring that policies and procedures include aspects of online safety, for example cyber-bullying is included in the anti-bullying policy and the Child Protection policy includes child grooming and sexting etc;

5.1.4. Working with the IT technicians to ensure that the filtering is set at the correct level for staff and children and inappropriate language or images;

5.1.5. Ensure staff training is provided on e-safety issues;

5.1.6. Ensure that e-safety is included in induction;

5.1.7. Monitor and evaluate incidents that occur to inform safeguarding developments.

6. Good Practice

6.1. E-Safety depends on effective practice at a number of levels:

6.1.1. Responsible computing and ICT use by all staff and pupils; encouraged by education and made explicit through published policies;

6.1.2. Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use;

6.1.3. Safe and secure broadband ensuring effective management of content filtering;

6.1.4. National Education Network standards and specifications.

7. Principles of the teaching and learning of e-safety

7.1. The purpose of using on-line technology in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school`s management information and business administration systems. Internet use is part of the statutory curriculum and a necessary tool for staff and pupils.

7.2. The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of the pupils including the blocking of any extremist material and inappropriate language or images.

7.3. In addition to using the internet in school, we recognise that children will use the internet and other digital technology in their own time at other locations and are at greater risk if they have not been taught what the dangers are and how to use them safely. Supporting and assisting the development of children's e-confidence and their ability to access the digital world effectively and safely is essential.

7.4. We acknowledge that the range of risks to young people in the digital environment is wide and ever changing e.g "grooming" by sexual predators via internet-enabled multi-player games is not uncommon.

7.5. At St Agnes C of E Voluntary Aided Primary School, we recognise the importance of raising the awareness of children so that they are able to keep themselves as safe as possible when using the internet and other digital technologies. In order to do this, we involve children and their parents/carers in the safe use of on-line technologies. Children are taught what on-line technology use is acceptable and what is not and are given clear objectives for its use. Children are educated in the effective use of on-line technology in research, including the skills of knowledge location, evaluation and retrieval. Lessons on e-safety are delivered half termly and our local PCSOs and LA provide input and scenarios regarding e-safety for the children to consider.

7.6. If staff or pupils discover unsuitable sites the URL (address) and contents must be reported to the Internet Service provider via the Computing Co-ordinator or ICT Technician. The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

7.7. We provide support and guidance to pupils and their parents/carers for the safe and responsible use of these on-line technologies. A partnership approach with parents is encouraged and guidance regarding e-safety is offered to parents in variety of different ways e.g information events, relevant links and documents available on the school website.

8. Personal mobile telephones and smart devices

8.1. The use of mobile phones (including taking photographs) by children is prohibited in school. If a child brings a mobile phone into school it will be confiscated and stored in a safe and inaccessible place in the classroom.

8.2. If a genuine need for a mobile is needed by a child (e.g. a Year 5 or 6 child walking home after school), this must be discussed with the headtecher by a parent or carer prior to the device entering school to see if extenuating curcumstances will be given. This mobile phone must then be delivered from the school office to be kept in a safe place at the start of each school day and collected at the end of the school day. Its use is still prohibited within the school grounds and the child and parent will be informed of this.

8.3. The use of smart watches or devices by children that can receive a mobile 2G/3G/4G or 5G signal, or wirelessly link itself with a signal such as Bluetooth or wi-fi to a mobile telephone stored in the school, is also prohibited.

8.4. Mobile phones must not be used for personal use by children or adults during lessons or formal school time.

8.5. The sending of abusive or inappropriate text messages, chat, messages or postings on social media is forbidden. Children should not have access to unlimited and unrestricted internet or means to use a mobile phone on the school premisis and thus this should not occur in school. Such issues occurring inside and outside school by children or adults will be investigated in line with the schools Behaviour, Child Protection and/or Diciplinary Policies.

8.6. Staff will be issued with a school phone where contact with pupils is required.

9. Acceptable Use

9.1. In order to prevent inappropriate situations occurring, it is important that staff, volunteers and children are aware of their responsibilities and the expectations whilst using technology. Each user signs a contract to ensure they know what is deemed “acceptable use of the internet”.

10. School Website

10.1. The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils’ home information will not be published. Website photographs that include pupils will be selected carefully. Pupils’ full names will not be used anywhere on the website, particularly in association with photographs.

10.2. Written permission from parents/carers will be obtained before photographs of pupils are published on the school website. The headteacher will take overall editorial responsibility and ensure content is accurate and appropriate.

11. Internet Access

11.1. The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. Internet access is planned to enrich and extend learning activities. Parents of all pupils are asked to sign and return a consent form giving permission for their child to use the internet.

11.2. In Foundation Stage and Key Stage 1, access to the internet is by adult demonstration and direct supervised access to specific, approved on-line materials.

11.3. In Key Stage 2, pupils use the internet for research purposes in addition to specific tasks. Pupils are taught the importance of e-safety and agree terms and conditions for acceptable internet use. Pupils are taught to be critically aware of the materials they read and are made aware that information may not always be reliable or accurate.

12. Educational benefits of the Internet

12.1. Benefits of using the Internet in education include:

12.1.1. Access to world-wide educational resources including museums and art galleries;
12.1.2. Educational and cultural exchanges between pupils world-wide;
12.1.3. Access to experts in many fields for pupils and staff;
12.1.4. Professional development for staff through access to national developments, educational materials and effective curriculum practice;
12.1.5. Collaboration across support services and professional associations;
12.1.6. Improved access to technical support including remote management of networks and automatic system update;
12.1.7. Access to tools of direct communication such as Video conferencing and email;
12.1.8. Exchange of curriculum and administration data with the Local Authority and DfE; access to learning wherever and whenever convenient.

13. Filters and Monitoring

13.1. In our responsibility to safeguard and promote the welfare of our children and provide them with a safe environment in which to learn, the school and governing body will work in partnership with parents, the Local Authority, the Department for Education and our internet service provider to ensure systems are in place to protect pupils are reviewed and improved.

13.2. The filtering strategy in school is selected to suit the age and curriculum requirements of the pupils of St Agnes C of E Primary School, including the blocking of extremist material and inappropriate language or images.

13.3. The school will do all that it reasonably can to limit children's exposure to risks from the school's IT system. As part of this process, the school leadership amd governing body will ensure the school has appropriate filters and monitoring systems in place.

13.4. The school leadership and governing body has considered the age range of our children, the number of children in school, how often they access the IT system and the proportionality of costs vs risks.

13.5. The appropriateness of the schools filters and monitoring systems will be informed in part, by the risk assessment required by the Prevent Duty. The school has looked at the UK Safer Internet Centre guidance, as well as using specialised external contractors, as to what "appropriate" filtering and monitoring might look like to help support filtering and moitoring in school.

14. Password Security

14.1. Password security is essential for staff as they are able to access and use pupil data. Staff are aware of their individual responsibilities to protect the security and

confidentiality of the school networks. Staff should ensure that computers and laptops are not left unattended.

15. Remote Learning

15.1. Keeping pupils, students and teachers safe during remote education is essential. Teachers delivering remote education online should be aware that the same principles set out in the school or college staff behaviour policy (sometimes known as a code of conduct) will apply.

15.2. All school and college staff should continue to act immediately (following their child protection policy and the processes set out in Part 1 of Keeping Children Safe in Education) if they have any concerns about a child or young person's welfare, whether the child or young person is physically in school or learning from home.

15.3. For support for parents and carers to keep their children safe online can be found at www.nspcc.org.uk/keeping-children-safe/online-safety (provided by the NSPCC) and www.parentinfo.org (from CEOP and Parent Zone) among other resources.

16. Video Conferencing and Livestreaming

16.1. Video conferencing or livestreaming can be used by school to host meetings, broadcast an event taking place in school or to view external events. It's a valuable educational medium which can connect our school with the community and with events outside of our locality.

16.2. Pupils are not permitted to use video conferencing or livestreaming equipment unsupervised.

16.3. Video conferencing or livestreaming equipment needs to be switched off when not in use.

16.4. The address/link or passwords to a video conference or livestream should not be made available on any website and should be changed regularly.

16.5. Pupils will not watch a livestream unsupervised in school but could possibly within remote learning or recreationally at home. To create a safe environment for pupils watching or engaging in a livestream, the children will be reminded:

- Not to share private information.
- Not to respond to contact requests from people they don't know.
- Who they should tell if they see or hear anything upsetting or inappropriate.

16.6. Hosting a livestream

Hosting a livestream means any situation where the school instigates, publishes and is responsible for streaming online content. This includes livestreaming lessons, assemblies, announcements, activities, and if external visitors livestream on the school site. When hosting a livestream the school will:

- Consider which platform to use since free platforms such as YouTube or Facebook Live do not allow you to restrict the audience.
- Consider inviting the audience to register to watch the stream and issue a login and password, or look into using a custom platform if livestreaming is regularly used within school.

- Ensure the privacy settings are appropriate and know how to report any offensive or abusive content.
- The stream will take place in school time and on school premises and will be supervised by appropriate adults at all times.
- Be sensitive to the needs of individual children who may be sensitive to certain topics or issues that may arise during the livestream.
- Appropriate staff will supervise and be on hand to handle any sudden changes or upsetting developments that may occur during the livestream.

16.7. Joining a livestream

When joining a livestream that is hosted by someone outside the school, the school recognised that participation through posting audio or written comments and liking or sharing the stream could be available. If the schools joins a livestream the teacher will:

- Familiarise themselves with the type of content to be used in the stream and check it is appropriate and relevant.
- Check with the provider on how they will use the stream in future. For example, will it be kept for archive purposes and will it be broadcast as a recorded event?
- Make sure pupils know they don't have to contribute to request donations on celebrity or vlogger streams.
- Remind pupils that any comments posted will be seen by others and cannot be edited or deleted and this can become a part of their digital footprint.

17. Email

17.1. Children may only use approved e-mail accounts on the school system. Children use class accounts that are restricted to communication within the school.

17.2. Children must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet someone.

17.3. Children are instructed to tell an adult if they receive an offensive e-mail.

17.4. E-mails sent to external organisations should be carefully written and authorised before sending, in the same way as a letter written on school headed notepaper.

17.5. The forwarding of chain letters is not permitted.

17.6. Access in school to external personal e-mail accounts may be blocked.

17.7. Passwords should be secure on the employee email system such as First Class.

18. Chat and Instant Messaging

18.1. Staff and pupils will not be allowed access to public or unregulated chat rooms. Pupils will not access social networking sites e.g. “Instagram”, “Snapchat”, “Facebook”. Pupils will only be allowed to use regulated educational chat environments if available. This will be supervised and the importance of chat room safety emphasised. Any forms of bullying or harassment is strictly forbidden and will be dealt with in line with the school’s behaviour policy.

18.2. To keep pupils safe at home, pupils are advised not to place personal photos on any social network space. Pupils are advised on security and encouraged to set

passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils are encouraged to invite known friends only and deny access to others.

19. Photographic, video and audio technology

19.1. It is not appropriate to use photographic or video devices in changing areas or toilets.

19.2. Care should be taken when capturing photographs or video to ensure that all pupils are appropriately dressed.

19.3. Staff may use photographic or video devices (including digital cameras, iPads and mobile phones) to support school trips and curriculum activities.

19.4. The downloading of audio and video files is not permitted without the prior permission of the e-safety lead and only in cases where they relate directly to the current educational task being undertaken.

19.5. Pupils should always seek permission of their teacher before making audio, photographic or video recordings within school grounds.

20. Emerging computing and ICT applications

20.1. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Emerging applications are encouraged to enhance learning and will be used in accordance with this policy.

21. Assessment of risk

21.1. In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils.

21.2. The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer.

21.3. Neither the school nor Oldham Local Authority can accept liability for material accessed or any consequences of internet access.

21.4. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

21.5. Methods to identify, assess and minimise risks will be reviewed regularly.

21.6. The Heateacher will ensure that the e-safety policy and Acceptable Use Policy is implemented and compliance with the policy is monitored.

22. Introducing the policy to pupils

22.1. Rules for acceptable use will be posted in all rooms where computers are used.

22.2. Pupils will be informed that Internet use will be monitored.

22.3. Instruction in responsible and safe use should precede internet access.

22.4. A lesson on responsible internet use covering both school and home use should be delivered half termly.

23. Introducing the policy to staff and volunteers

23.1. All staff and volunteers must accept the terms of responsible internet use statement before using any internet resource in school.

23.2. All staff including teachers, supply staff, classroom assistants, administration caretaking staff and Governors will be provided with the School Internet policy and its importance explained.

23.3. Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

23.4. The monitoring of internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by the SLT.

23.5. Staff development in safe and responsible Internet use, including familiarisation of the e-safety and acceptable use policy will be provided as required.

24. Introducing the policy to parents

24.1. Parents' attention will be drawn to the School e-Safety Policy in the Friday Note and on the School Web site.

24.2. Parent's need to give permission for children to use the Internet.

24.3. Parents need to give permission to have any photographs published of their children on the Website.

25. Maintaining ICT system security

25.1. The school is directly responsible for ensuring we have the appropriate level of security protection procedures in place, in order to safeguard their systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies.

25.2. The school ICT systems will be reviewed regularly with regard to security.

25.3. Virus protection will be installed and updated regularly.

25.4. Personal data sent over the internet will be encrypted or otherwise secured. All personal devices will be encrypted by the ICT team.

25.5. Unapproved system utilities and executable files will not be allowed in pupils` work areas or attached to e-mail.

25.6. Files held on the school`s network and the cloud will be regularly checked.

25.7. The ICT Leader/ICT technicians will ensure that the system has the capacity to take increased traffic caused by internet use.

25.8. Further guidance on e-security will be sought from the National Education Network. In addition, broader guidance on cyber security including considerations for governors and trustees will be found at www.ncsc.gov.uk .

26. The responses necessary when a risk to a child is discovered

26.1. Prompt action is required if a complaint is made regarding the use of on-line technology. The facts of the case must be established and presented to the e-safety lead. A minor transgression of the rules may be dealt with the teacher as part of normal class discipline. Other situations could be potentially more serious and a range of sanctions will be used, linked to the Behaviour Policy.

26.2. Complaints of a child protection nature will be dealt with in accordance with Oldham Local Safeguarding Children's Partnership child protection procedures. Any complaints regarding staff misuse must be referred directly to the headteacher (or in the case of the headteacher, the chair of governors).

26.3. Equal Opportunities

26.4. Provision is made for all children regardless of ability, disability, additional needs, medical conditions, gender, faith or ethnicity and reasonable adjustments are made in a range of ways. All children have a right to be treated equally and the school will take measures against those who do not abide by this ethos.

27. Monitoring and Evaluation

27.1. Technology, and risks and harms related to it evolve and changes rapidly. Policy and practice is monitored and evaluated on a regular basis. The school will carry out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face. The school will use an online safety self-review tool for schools such as those found found via the 360 safe website.

27.2. Monitoring may also take the form of lesson observations, planning and book scrutiny, questionnaires, discussions with children or learning walks. Feedback will be given to all staff along with recommendations to inform future policy and planning.

27.3. The school leadership team have a responsibility to ensure the policy is embedded into the school provision and report to governors on the effectiveness of the policy. The governors may also ask further questions, such as UKCIS Questions from the governing board, which can be used by the governors to gain a basic understanding of the current approach to keeping children safe online.

28. How to respond if a risk is discovered

28.1. The e-safety lead will ensure that an adult follows these procedures in the event of any misuse of the internet:

28.1.1. An inappropriate website is accessed inadvertently:

28.1.1.1. Report website to the e-safety lead.
28.1.1.2. Contact the filtering service so that the site can be added to the banned or restricted list.
28.1.1.3. Log the incident.

28.1.2. An inappropriate website is accessed deliberately:

28.1.2.1. Report website to the e-safety lead.
28.1.2.2. Log the incident.
28.1.2.3. Report to the headteacher and e-safety lead immediately.
28.1.2.4. Headteacher to refer to Acceptable Use Rules and follow agreed actions for discipline.
28.1.2.5. Inform the filtering services in order to reassess the filters.

28.1.3. An inappropriate website is accessed deliberately by a child or young person:

28.1.3.1. Refer to the Acceptable Use rules that were agreed.
28.1.3.2. Reinforce the knowledge that it is illegal to access certain images and that the police can be informed.
28.1.3.3. Log the incident.
28.1.3.4. Decide on appropriate sanction.
28.1.3.5. Notify the parent/carer.
28.1.3.6. Contact the filtering to notify them of the website.

28.1.4. An adult receives inappropriate material:

28.1.4.1. Do not forward this material to anyone else – doing so could be an illegal activity.
28.1.4.2. Alert the headteacher immediately.
28.1.4.3. Ensure the device is removed and log the nature of the material.
28.1.4.4. Contact relevant authorities for further advice e.g police, social services, CEOP.
28.1.4.5. Log the incident.

28.1.5. An illegal website is accessed or illegal material is found on a computer. (The following incidents must be reported directly to the police):

28.1.5.1. Indecent images of children found. (Images of children whether they are cartoons of children or young people apparently under the age of 16 involved in sexual activity or posed in a sexually provocative manner).
28.1.5.2. Incidents of “grooming” behaviour.
28.1.5.3. The sending of obscene materials to a child.
28.1.5.4. Criminally racist or anti-religious material.
28.1.5.5. Violent or bomb making material.
28.1.5.6. Software piracy.
28.1.5.7. The promotion of illegal drug taking.
28.1.5.8. Adult material that potentially breaches the Obscene Publications Act in the UK.

28.1.5.9. If any of these are found, the following should occur:

28.1.5.10. Alert the headteacher or the deputy designated person for child protection immediately.

28.1.5.11. DO NOT LOG OFF the computer or disconnect from the electricity supply.
28.1.5.12. Contact the police and or CEOP and social care immediately.
28.1.5.13. If a member of staff or volunteer is involved, refer to the allegations against staff policy and report to the Local Authority Designated Officer. The Local Authority Designated Officer (LADO) for Oldham Local Safeguarding Children's Partnership is Colette Morris, telephone number: 0161 770 8870 or mobile: 07583101863. The LADO Support Officer can be reached on 0161 770 8081.

28.1.6. An adult has communicated with a child or used ICT equipment inappropriately (e- mail/text messages etc):

28.1.6.1. Ensure the child is reassured and remove them from the situation.
28.1.6.2. Report to the headteacher or the deputy designated person for child protection immediately who will then follow the Allegations Procedure and child protection procedures.
28.1.6.3. Report to the Local Authority Designated Officer. The Local Authority Designated Officer (LADO) for Oldham Local Safeguarding Children's Partnership is Colette Morris, telephone number: 0161 770 8870 or mobile: 07583101863. The LADO Support Officer can be reached on 0161 770 8081.
28.1.6.4. Preserve the information received by the child if possible.
28.1.6.5. Contact the police as necessary.

28.1.7. Threatening or malicious comments are posted to the school website or other online platform (or printed out) about an adult in school :

28.1.7.1. Preserve any evidence and log the incident.
28.1.7.2. Inform the headteacher immediately and follow Child Protection policy.
28.1.7.3. Inform the e-safety lead so that new risks can be identified.
28.1.7.4. Contact the police or CEOP as appropriate.

28.1.8. Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted this should be reported to the headteacher.

28.1.9. Threatening or malicious comments are posted to the school website or learning platform about a child in school or malicious text messages are sent to another child/young person (cyber bullying)

28.1.9.1. Preserve any evidence and log the incident.
28.1.9.2. Inform the headteacher immediately.
28.1.9.3. Check the filter if an internet based website issue.
28.1.9.4. Contact parent/carers.
28.1.9.5. Refer to the anti-bullying policy.
28.1.9.6. Contact the police or CEOP as necessary.

29. Protecting Personal Data

29.1. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 (DPA 2018).

29.2. The procedures and practice created by this policy have been reviewed in the light of our Data Protection Policy.

29.3. All data will be handled in accordance with the school's Data Protection Policy.

Data Audit For This Policy					
What ?	**Probable Content**	**Why ?**	**Who ?**	**Where ?**	**When ?**
Child's Name	Name	Log-in Information	All Staff (Where Necessary) Parents Children	Kept in children's file or shredded.	Kept in children's file or sent home.

29.4. As such, our assessment is that this policy :

Has Few / No Data Compliance Requirements	**Has A Moderate Level of Data Compliance Requirements**	**Has a High Level Of Data Compliance Requirements**
		✓