



Online Safety Policy & Agreement 2026

Last Reviewed: May 2026

Last Approved by P Seery

Next Review Date: June 2027

Person responsible for the monitoring, evaluation and implementation of this document: P Seery

1. Rationale

- 1.1. Alder Grange School welcomes the development of new technologies for communicating, creating, and learning—including **Artificial Intelligence (AI) and cloud-based platforms like Google Workspace for Education**. We will use them wherever they are appropriate to enhance the work done with the pupils at school.
- 1.2. All members of our school community must recognise our responsibility to take reasonable measures to ensure that the risks of harm to young people's welfare are minimised, **including risks associated with algorithmic bias, misinformation, and AI-generated content**.
- 1.3. Alder Grange School also recognises the need to protect staff and volunteers from inappropriate conduct from young people in their personal lives and from situations that may make them vulnerable to allegations of wrongful conduct.
- 1.4. Use of any of this technology requires appropriate conduct in public spaces outside our work and in our personal lives and this includes any form of electronic communication

2. Monitoring the effectiveness of this policy

- 2.1. Alder Grange will monitor the effectiveness of this policy through:
 - 2.1.1. Logs of reported incidents
 - 2.1.2. Monitoring logs of internet activity (including sites visited) / filtering
 - 2.1.3. Internal monitoring data for network activity
 - 2.1.4. Surveys / questionnaires of students / pupils / parents / carers / staff

3. Scope of the policy

- 3.1. This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.
- 3.2. The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other negative online activities.
- 3.3. The 2011 Education Act increased the Head teacher's powers with regard to the searching of electronic devices and the deletion of data which may cause offence or distress providing this forms part of the school Behaviour Policy. Alder Grange will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

4. Roles and Responsibilities

4.1. Governors

Governors are responsible for the ratification of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out at Governors Welfare Meetings where governors will have information about incidents and online safety and monitoring reports. The link Governor for Safeguarding will also have direct links to e-safety within school via these meetings.

4.2. Headteacher

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility or online safety will be delegated to the Designated Safeguarding Lead and the ICT Manager. The Head teacher and the Designated Safeguarding Leads are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. This is also covered in the School Safeguarding Policy

4.3. Critical Incidents

Alder Grange's DSL takes day to day responsibility for online safety issues and has leading role in establishing and reviewing the school online safety policies / documents. However, in the event of a serious online incident the relevant parts of the critical incident procedures may be followed. The Designated Safeguarding Lead will ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and will provide training and/or advice for staff. This will also cover liaison with the Local Authority / relevant body / school technical staff.

4.4. The Designated Safeguarding Lead

The DSL at Alder Grange receives daily reports of online safety incidents and will keep a log of significant incidents to inform any future online safety developments. The DSL will also report significant issues to Senior Leaders. (Alder Grange currently uses Smoothwall Safeguarding filtering). The DSL is responsible for ensuring that all staff have the required knowledge and understanding of safeguarding issues related to e-safety.

4.5. The ICT Manager / ICT Staff: The ICT Manager is responsible for ensuring that:

The school's technical infrastructure is secure and is not open to misuse or malicious attack

The school meets required online safety technical requirements and any Local Authority Guidance that may apply

Users may only access the networks and devices through a properly enforced password protection policy

The filtering policy is applied and updated on a regular basis so that it is compliant with online safety statutory requirements

The use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to Senior Leaders for investigation and subsequent action / sanction;

Monitoring software / systems are implemented and updated as agreed.

4.6 Teachers and Support Staff

Are responsible for ensuring that:

They have an up-to-date awareness of online safety matters and of the current Safeguarding Policies and practises;

They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP);

They report any suspected misuse or problem to the DSL for investigation and action/sanction;

All digital communications with students / pupils / parents / carers / governors should be on a professional level and only carried out using official school systems;

Online safety issues are embedded in all aspects of the curriculum and other activities

Students / pupils understand and follow the E-Safety Policy and acceptable use policies;

Students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;

Are responsible for ensuring that they monitor the use of digital technologies and AI tools in lessons. They must guide students on the ethical use of AI to prevent plagiarism and ensure

academic integrity.

They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.

4.7 Pupils

Are responsible for using school digital technology systems in accordance with the Pupil Acceptable Use Agreement. They must also:

Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;

Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;

Be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying;

Understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the Alder Grange's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Must have a good understanding of research skills and the need to avoid plagiarism, including passing off AI-generated content (e.g., from ChatGPT, Gemini) as their own original work.

4.8 Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Alder Grange School will take every opportunity to help parents understand these issues through parents' evenings, Newsletters, letters, website and parent mail information about relevant national or local online safety campaigns

Parents and carers are encouraged to support Alder Grange School by promoting good online safety practice and to follow guidelines on the appropriate use of:

Digital and video images taken particularly when allowed at school events;

Access to parents' sections of the website;

Their children's personal devices in school, where this is allowed;

Search websites to ensure appropriate content is accessed.

5. Education

- 5.1. Whilst regulation and technical solutions are very important, their use must be balanced by educating all pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.
- 5.2. Online safety is a focus where relevant in all areas of the curriculum and staff reinforce online safety messages across the curriculum. This includes:
- 5.3. A planned online safety curriculum as part of Computing lessons and this is regularly revisited;
- 5.4. Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities where appropriate.
- 5.5. Pupils are taught in all lessons to be critically aware of the materials and content they access on-line and are encouraged to always validate the accuracy of information, particularly recognising that AI tools can produce "hallucinations" or factually incorrect information.
- 5.6. Pupils are taught to acknowledge the source of information used, including properly citing when AI tools have been used to assist in brainstorming, translating, or structuring work.
- 5.7. Pupils are helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- 5.8. Staff should always act as good role models in their use of digital technologies the internet and mobile devices
- 5.9. In lessons where internet use is pre-planned, it is best practice that pupils be guided to sites checked as suitable for their use. There are processes in place for dealing with any unsuitable material that is found in internet searches.
- 5.10. Where pupils are allowed to freely search the internet, staff must be vigilant in monitoring the content of the websites the young people visit.
- 5.11. It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g., racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study.

Any request to do so, should be auditable, with clear reasons for the need.

6. Technical Infrastructure (Equipment, Filtering and Monitoring)

6.1. The Head teacher and designated staff are responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that procedures approved within this policy are implemented.

6.2. The Head teacher will also ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities: This will mean:

There will be regular reviews of the safety and security of school technical systems to ensure that the subsequent safeguarding / technical requirements of the system are met;

Servers, wireless systems and cabling is securely located and physical access restricted;

All users have clearly defined access rights to school technical systems and devices;

All users will be provided with a username and secure password by the Network Manager who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password and should change their password periodically and at least annually.

The “master / administrator” passwords for the school ICT system, used by the ICT Manager (or other person) must also be available to the Head teacher or other nominated senior leader and kept in a secure place.

6.3. The ICT Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.

6.4. Internet access is filtered for all users. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes

6.5. Internet filtering ensures that children are safe from terrorist and extremist material when accessing the internet.

6.6. Alder Grange technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.

6.7. The CPOM (Child Protection Online Management) system is in place for all staff to report any incidents of concern to the Designated Safeguarding Lead

6.8. Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date virus software.

- 6.9. Temporary log on codes are provided by the ICT Manager for the provision of temporary access of “guests” (e.g., trainee teachers, supply teachers, visitors) onto the school systems.
- 6.10. Staff and pupils are prohibited from download executable files (.exe) onto the school system and installing programs.
- 6.11. Removable media carrying sensitive or confidential information should be encrypted. (e.g., memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

7. Digital and Video Images

- 7.1. The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet.
- 7.2. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place.
- 7.3. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and always seek permission from parents or carers where digital images are sought.
- 7.4. When using digital images, staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g., on social networking sites such as Snapchat, Instagram and Facebook.
- 7.5. Parents/Carers are asked to ‘opt in’ to publicity via a consent form at the start of school. Parents/Carers have the option to opt out at any time by informing the school office.

8. Data Protection

- 8.1. Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations, and subsequent reforms which states that personal data must be:

Fairly and lawfully processed

Processed for limited purposes

Adequate, relevant and not excessive

Accurate

Kept no longer than is necessary

Processed in accordance with the data subject's rights

Secure

Only transferred to others with adequate protection

8.2. Staff must ensure that:

At all times they take steps to ensure the safe keeping of personal data, minimising the risk of its loss or misuse

They use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data

Transfer sensitive data using encryption and secure password protected devices

Staff must not use USB sticks in school, unless with prior permission of Head Teacher, and under supervision of IT Manager

Use of cloud technologies must be used with the same regard to confidentiality and data loss

Use of cloud technologies and AI platforms must be used with a strict regard to confidentiality and data loss.

- Staff and pupils must never input sensitive, personal, or identifiable school data into public generative AI tools (e.g., public ChatGPT or public Gemini), as this data may be used to train external models.

8.3. When personal data is stored on any portable computer system, or any other removable media:

The data must be encrypted and password protected

The device must be password protected

The device must offer approved virus and malware checking software

The data must be securely deleted from the device, once it has been transferred or its use is complete

9. Communications

9.1. This is an area where a wide range of rapidly developing technologies and uses has the potential to enhance learning.

9.2. When using communication technologies Alder Grange School considers the following as good practice

- 9.3. The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with each other.
- 9.4. Users must immediately report to the Designated Safeguarding Lead – in accordance with the school Safeguarding Policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- 9.5. Any digital communication between staff and students / pupils or parents / carers / governors (email, social media, chat, blogs) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- 9.6. All pupils are taught about online safety issues, such as the risks attached to the sharing of personal details. They are also taught strategies to deal with inappropriate communications and are reminded of the need to communicate appropriately when using digital technologies.
- 9.7. Personal information should not be posted on the school website or Facebook page and only official email addresses should be used to identify members of staff.

10. Social Media - Protecting Professional Identity

- 10.1. Alder Grange recommends the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

Ensuring that personal information is not published

Training is provided including: acceptable use; social media risks; reporting issues

There is clear reporting guidance, including responsibilities, procedures and Sanctions

No reference should be made in social media to pupils, parents / carers or school staff

The school members do not engage in online discussion on personal matters relating to members of the school community

Personal opinions are not to be attributed to the school or local authority;

- 10.2. Security settings on personal social media profiles are encouraged to be regularly checked to minimise risk of loss of personal information.

- 10.3. The school's use of social media for professional purposes will be checked regularly by the Headteacher to ensure the compliance of school policies.

10.4. If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.

11. Illegal Activities

11.1. In the event of an illegal activity the Head of School, Assistant Head Teacher (Behaviour) and/or the DSL should be notified immediately.

11.2. Child sexual abuse images

The taking, making, distributing or publishing of an indecent image, contrary to Section 1 of the Protection of Children Act 1978

Possession of an indecent image, contrary to Section 160 of the Criminal Justice Act 1988 III.

Possession of a prohibited image of a child, contrary to Section 62 of the Coroners and Justice Act 2009 (dealing specifically with non-photographic

Images not covered by s. 1 PCA 1978 or s. 160 CJA 1988, and including computer-generated images (CGI's), cartoons, manga images and drawings).

11.3. Specific 'Grooming' Offences contrary to the Sexual Offences Act 2003

Causing or inciting a child to engage in sexual activity

Causing a child to watch a sexual act

Arranging and facilitating a child sex offence

Sexual communication with a child (where a communication is 'sexual' if any part of it relates to sexual activity, or a reasonable person would, in all the circumstances but regardless of any person's purpose, consider any part of the communication to be sexual).

11.4. Pornography: Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character), contrary to Section 63 of the Criminal Justice and Immigration Act 2008.

11.5. Stirring up Racial Hatred contrary to Part III of the Public Order Act 1986: Displaying, publishing or distributing written material, visual images or sounds, which are intended to stir up racial hatred or, having regard to all the circumstances, such hatred is likely to be stirred up thereby.

11.6. **Other activities** e.g., cyber-bullying would be banned and could lead to criminal prosecution.

12. User Permissions and Internet/System Usage

Users of Alder Grange systems (including staff) must not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	
	Level of Acceptability/Illegality
Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978	Unacceptable & Illegal
Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.	Unacceptable & Illegal
Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Public Order Act 1986	Unacceptable & Illegal
Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986	Unacceptable & Illegal
Pornography	Unacceptable & potentially illegal
Promotion of any kind of discrimination	Unacceptable and potentially illegal
Threatening behaviour, including promotion of physical violence or mental harm	Unacceptable and potentially illegal
Promotion of extremism or terrorism	Unacceptable and Illegal
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute	Unacceptable

Using school systems to run a private business	Unacceptable
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy	Unacceptable
Infringing copyright	Unacceptable
Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords)	Unacceptable
Creating or propagating computer viruses or other harmful files	Unacceptable
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)	Unacceptable
On-line gaming (educational)	Acceptable at certain times
On-line gaming (non-educational)	Unacceptable
On-line gambling	Unacceptable
On-line shopping / commerce (non-school related)	Unacceptable
File sharing	Acceptable for nominated users with permissions
Use of social media (FaceBook/Twitter)	Acceptable for nominated users with permissions to access school social media account only
Use of messaging apps (WhatsApp/Messenger/SMS)	Unacceptable

Use of video broadcasting e.g., YouTube	Unacceptable
Creating or distributing AI-generated "Deepfakes" or manipulated media to harass or impersonate others	Unacceptable & Illegal
Using Generative AI to bypass academic integrity (Plagiarism / cheating on coursework)	Unacceptable
Inputting private or confidential school data into unauthorised public AI chatbots	Unacceptable

13. Procedures

13.1. In the event of accidental infringement or suspicion, all steps in this procedure should be followed:

Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

Conduct the procedure using information from Smooth wall Safeguarding or a designated computer that will not be used by pupils and, if necessary, can be taken off site by the police should the need arise. On occasion it may be necessary to confiscate an electronic device carried by a pupil.

Records of the URL of any site containing the alleged misuse and a description of the nature of the content causing concern must be kept. It may also be necessary to record and store screenshots of the content from the device under investigation. The ICT technicians will normally be asked to do this.

These may be printed, signed and attached to any incident form (except in the case of images of child sexual abuse – see below).

Once this has been completed and fully investigated the Head teacher will need to judge whether this concern has substance or not.

If it does then appropriate action will be required and could include the following: Internal response or discipline procedures;

Involvement by Local Authority or other organisation (as relevant)

Police involvement and/or action.

If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately.

13.2. Other instances to report to the police would include:

Incidents of 'grooming' behaviour

The sending of obscene materials to a child

Adult material which potentially breaches the Obscene Publications Act

Criminally racist material

Promotion of terrorism or extremism;

Other criminal conduct, activity or materials.

14. Social Media Guidelines

- 14.1. Below are guidelines for the use of social media and other internet forums for pupils. This applies to use on school computers, and on personal devices both in and out of school hours.
- 14.2. To that end, this Policy outlines the guidelines and behaviours that all users are expected to follow.
- 14.3. Pupils are expected to follow the same rules for good behaviour and respectful conduct online as offline
- 14.4. Misuse of social media can result in disciplinary sanctions.
- 14.5. While social networking is fun and valuable, there are some risks you should keep in mind when using these tools. In the social media world, the lines are blurred between what is public or private.
- 14.6. You must know and follow the school's Behaviour policy and internet usage policy.
- 14.7. Regardless of your privacy settings, assume that all of the information you have shared on your social network is public information.
- 14.8. Always treat others in a respectful, positive and considerate manner online as you would offline.
- 14.9. Don't share confidential information.
- 14.10. Do not publish, post or release information that is considered confidential or not public. If it seems confidential, it probably is. Online "conversations" are never private. Do not use your birth date, address, and mobile phone number on any public website.
- 14.11. To ensure your safety, be careful about the type and amount of personal information you provide. Avoid talking about personal schedules or situations.
- 14.12. NEVER give out or transmit personal information of other pupils or adults.
- 14.13. Respect brand, trademark, copyright information and/or images of the school.
- 14.14. It is generally not acceptable to post pictures of other pupils without the expressed written consent of their parents.
- 14.15. Sending electronically or sharing naked pictures is illegal and even if you send pictures of yourself, you risk a criminal record, particularly if you are under 16.
- 14.16. Pictures shared outside school hours, but of or by pupils, can still be referred to school and school will employ sanctions in line with the behaviour policy if needed.
- 14.17. Pay attention to the security warnings that pop up on your computer before clicking on unfamiliar links. They actually serve a purpose and protect you and the school.

- 14.18. When using Twitter, Facebook, Snapchat, Instagram and other tools or social media platforms, be sure to follow their printed terms and conditions
- 14.19. Be sure to correct any mistake you make immediately, and make it clear what you've done to fix it
- 14.20. Apologise for the mistake if the situation warrants it
- 14.21. If it's a MAJOR mistake (e.g., exposing private information or reporting confidential information), please let someone know immediately so the school can take the proper steps to help minimise the impact it may have.
- 14.22. Users should always use the Internet, network resources, and online sites in a courteous and respectful manner.
- 14.23. Users should also recognise that among the valuable content online is unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research via the Internet.
- 14.24. Users should also remember not to post/share anything online that they wouldn't want parents, teachers, or future colleges or employers to see. Once something is online, it's out there— and can sometimes be shared and spread in ways you never intended. You may also unknowingly be breaking the law.
- 14.25. If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, or the safety of another pupil, bring it to the attention of an adult (teacher or staff if you're at school; parent if you're using the device at home) immediately. XXI. Cyberbullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyberbullying. Don't be mean. Don't send emails or post comments with the intent of scaring, hurting, or intimidating someone else. Using social media to be racist, homophobic or sexist or to share views of others who express these views is unacceptable, even outside of school hours, and sanctions will be employed in line with the school behaviour policy. Cyberbullying will be treated in the same way as bullying in person. This applies to comments made about pupils and/or staff.
- 14.26. Engaging in these behaviours, or any online activities intended to harm (physically or emotionally) another person, will result in disciplinary sanctions and loss of ICT privileges. In some cases, cyberbullying can be a crime. We will refer to the Police if needed, and work with them to agree to sanctions. Remember that your activities are monitored and retained by others.
- 14.27. School staff are not allowed to message or 'friend' pupils on social media whilst they are on roll and for 5 years after they have left. Pupils should report any concerns they have related to this in school.
- 14.28. This is not intended to be an exhaustive list. Users should use their own good judgement when using social media.
- 14.29. Users must not use AI tools to generate and post fake images, audio, or video of other students or staff members on any social media or messaging platforms. This form of cyberbullying is strictly

prohibited and may result in police involvement.

Appendix 1: Pupil Internet Usage Agreement

INTRODUCTION: Alder Grange owns the ICT system. It is made available to students because the school wants to give them the best educational experience and to open up as many appropriate sources of learning as possible. The ICT system, and the Internet in particular, offers considerable opportunities for this.

However, it opens up several dangers for those who do not fully understand how it works and the law regarding the use of the Internet is increasingly complex. This Agreement has been drawn up, after much careful thought and consultation, to protect all parties – students, staff and the school.

THE AGREEMENT

1. The school is legally responsible for all ICT and Internet activity carried out on its hardware and software. The school reserves the right to monitor any Internet sites visited.
2. The school reserves the right to examine and delete any files that may be held on aldergrange.com domain.
3. Therefore, all system users should study, accept and sign this Agreement and return it to the ICT Curriculum Leader (Failure or refusal to do so **must** result in denial/withdrawal of Internet and/or ICT access).
4. All Internet activity should be appropriate to the educational work being done.
5. Access to the Internet may only be made through the authorised account and password.
6. Under NO circumstances should one student's password be revealed to, or used by another person.
7. Under no circumstances must a student access another person's file.
8. Any activity that threatens the integrity of the school ICT system(s), or activity which threatens or corrupts other systems, is strictly forbidden (including importing disks, CDs, Pen Drives or other files unless permission is granted in advance).
9. Users are responsible for all email sent, and for contacts made that may result in email being received. Students must abide by the safety guidelines laid down.
10. Use for personal financial gain, gambling, political purposes or advertising, is forbidden.
11. The ordering of chargeable items over the Internet is forbidden and any costs incurred through inappropriate use of the Internet will be recovered from the student or their parent or carer.
12. Copyright of all materials (whether printed or otherwise performed) must be respected.
13. Posting anonymous messages and forwarding "chain" letters/messages is forbidden.
14. The sending of offensive e-mails is forbidden and will be treated as the criminal offence it is.

15. Any and all emails to a member of staff must be sent via the school email system.
16. All current guidelines regarding students' safety and confidentiality must be followed at all times. This will normally include **not**:
 - (a) giving a home address, telephone or mobile 'phone number;
 - (b) arranging to meet someone unless a parent, carer or teacher has agreed.
17. School staff may check all files and may monitor the Internet sites visited.
18. Contacting staff via personal email is strictly forbidden unless sanctioned in advance by the Headteacher. The sending of any inappropriate email will be treated as a serious offence.
19. The highest standards must be observed in all messages sent via the Internet, as they may be forwarded inadvertently or incorrectly and may not be retrieved – any unpleasant material or messages received must be reported, confidentially, to help protect **all** students.
20. The use of the network to access inappropriate materials such as pornographic, extremist, racist or offensive material is forbidden.
21. As listed in the E-Safety Policy the use of the network to stir up hatred on the grounds of religious, racial, or sexual orientation is forbidden.
22. As listed in the E-Safety Policy the use of the network to cyber-bully is banned and could lead to criminal prosecution.
23. Buying anything over the Internet from a school account is prohibited.
24. I understand that the use of Artificial Intelligence (AI) to generate essays, homework, or coursework without the explicit permission of my teacher is a breach of academic integrity. If I use AI to assist me, I must properly cite it and declare its use.
25. I will not create, share, or distribute any AI-generated manipulated media (such as "deepfakes") of any staff, pupil, or member of the school community.

This agreement should be regarded as legally binding. Failure to keep to the agreement may lead to the immediate withdrawal of Internet and ICT access to the user, and legal proceedings.

Google Workspace for Education Account

Your child will be provided access to a **Google Workspace for Education** account (formerly G Suite). This means that they will have access to a set of secure educational productivity tools including Google Docs, Drive storage, Google Classroom, and approved Google AI learning integrations.

Pupils can use their Google Workspace account on any device inside or outside of school by signing in via this website: <https://www.google.co.uk/>. This will allow them to access their school documents and resources outside of school and return homework through Google Classroom.

Security and AI Privacy:

Please note that all documents and information created through Google Workspace for Education are secured within Alder Grange's walled-garden domain. They cannot be shared outside of this Alder Grange account without permission.

- **Data Privacy:** We only supply a name and email address to Google for your child to use these services. Google Workspace for Education guarantees that school data, student files, and emails are **never used to train Google's public AI models** or used for advertising purposes.
- Information regarding privacy of data can be viewed here:
https://workspace.google.com/terms/education_privacy.html

In order to use Google Workspace for Education and to comply with GDPR rules, we require your consent for your child to use these services.

If you have any further questions regarding this, please contact the school using the email address: reception@aldergrange.com or telephone the school.

RESPONSIBLE INTERNET USE

Student Full Name (print):

Form:

STUDENT AGREEMENT

I have read and understand the Internet Use Agreement. I will use the computer system and Internet in a responsible way and obey these rules at all times.

Signed: Date:

PARENT'S OR GUARDIAN'S CONSENT FOR INTERNET ACCESS AND A GOOGLE CLASSROOM ACCOUNT

I have read and understood the Internet Use Agreement for Students and give permission for my son/daughter to access the Internet and Google Classroom. I understand that the school will take all reasonable precautions to ensure students cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed: Date:

Please print name:

.....
...

Relationship to

child:.....
.....

Please sign and return to the school office