ALDER GRANGE SCHOOL

SECTION H
WELFARE COMMITTEE: SAFEGUARDING

(Governors' Welfare Committee)

F1 .3 E-SAFETY

Reviewed & approved by Governors' Welfare Committee: January 2020
Next review: January 2021

The person responsible for the monitoring, evaluation and implementation of this document: Mr D Birtles

Table of Contents

Rationale

Alder Grange School welcomes the development of new technologies for communicating and learning and will use them wherever they are appropriate to enhance the work done with the pupils at school.

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; and, where there are concerns about young peoples' welfare, to take appropriate actions to address those concerns.

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.

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. Due to the ever changing nature of digital technologies, it is best practice that we review this E-Safety Policy at least annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

Monitoring the effectiveness of this policy

Alder Grange will monitor the effectiveness of this policy through:

- Logs of reported incidents;
- Monitoring logs of internet activity (including sites visited) / filtering;
- Internal monitoring data for network activity;
- Surveys / questionnaires of students / pupils // parents / carers // staff.

Scope of the policy

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.

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. 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.

This policy also dovetails with the school Safeguarding Policy and the Behaviour and Anti-bullying policies.
F10.1 Positive Behaviour for Learning and Personal Achievement
F10.5 Anti Bullying Policy
F1.1 Safeguarding Policy
F1.3 Social Media Policy
H5.3 Internet Usage (Pupils and Staff)

1. Roles and Responsibilities

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. This will form a fixed agenda item at these meetings. The link Governor for Safeguarding will also have direct links to e-safety within school via these meetings.

Head teacher
The Head teacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for 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.

Critical Incidents
Alder Grange's DSL takes day to day responsibility for online safety issues and has a 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.

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.

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.

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;
- 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;

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.

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.

2. Education

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.

Online safety is a focus where relevant in all areas of the curriculum and staff reinforce online safety messages across the curriculum.

This includes:

- A planned online safety curriculum as part of Computing lessons and this is regularly revisited;
- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities where appropriate.

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.

Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

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.

Staff should always act as good role models in their use of digital technologies the internet and mobile devices.

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.

Where pupils are allowed to freely search the internet, staff must be vigilant in monitoring the content of the websites the young people visit.

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.

3. Technical Infrastructure (Equipment, Filtering and Monitoring)

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.

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.

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.

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

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

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.

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

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.

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.

Staff and pupils are prohibited from download executable files (.exe) onto the school system and installing programs.

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.

Digital and Video images

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.

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.

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.

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.

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.

4. Data Protection

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.

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 are no longer able to use USB sticks in school
- Use of cloud technologies must be used with the same regard to confidentiality and data loss

When personal data is stored on any portable computer system, memory stick 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.

5. Communications

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

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

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.

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.

Any digital communication between staff and students / pupils or parents / carers / governors (email, social media, chat, blogs, VLE etc.) 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.

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.

Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

6. Social Media - Protecting Professional Identity

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

Also, please see full **Social Media Policy**

Personal Use:

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy. Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

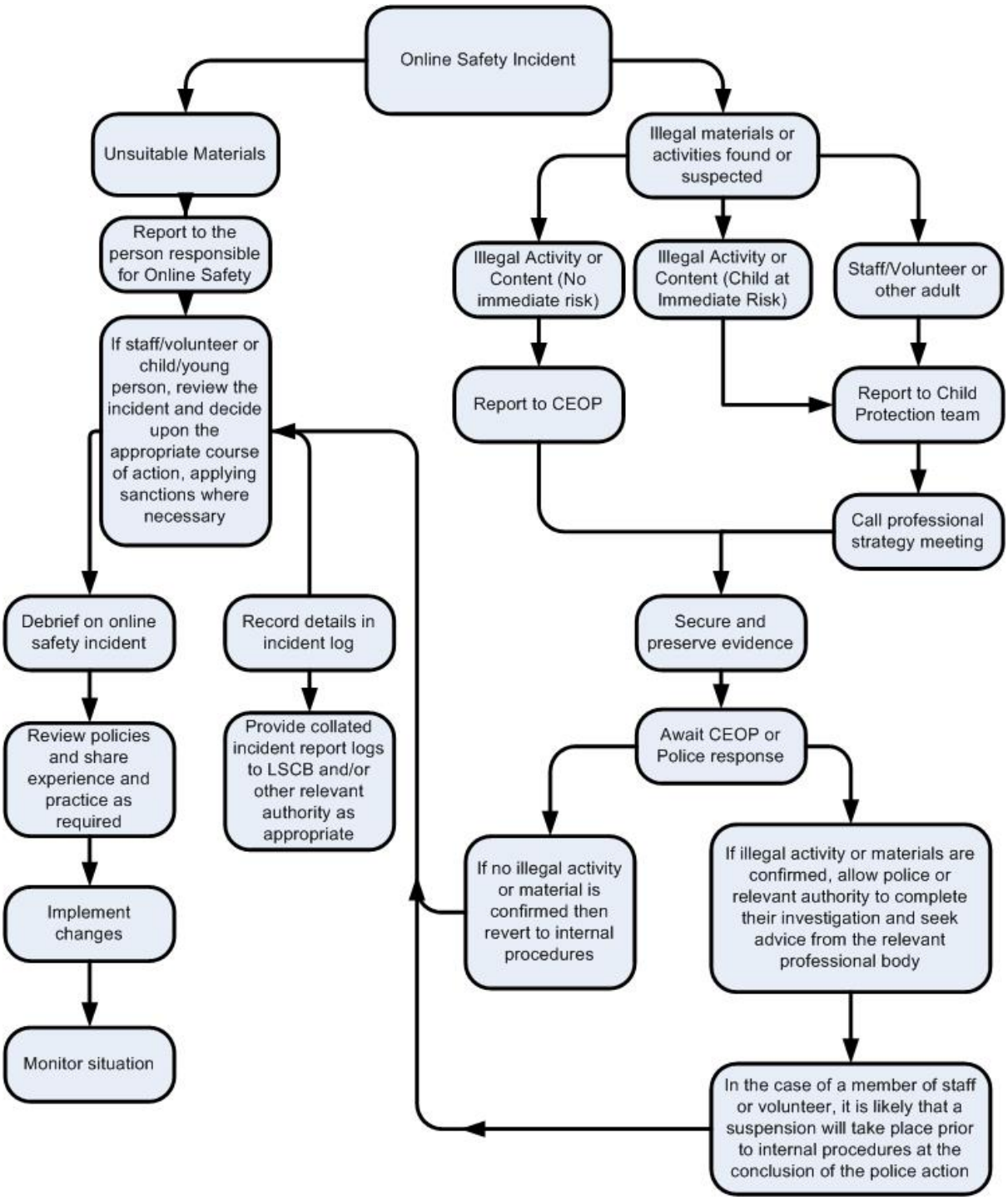
Monitoring of Public Social Media

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

Illegal Incidents

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.

7. Flowchart


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
Implement changes
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

8. Illegal Activities include, but are not limited to:

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**
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.)

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).

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**.

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.

Stirring up Hatred on Religious Grounds or Grounds of Sexual Orientation, contrary to Part 3A of the Public Order Act 1986
Possessing, displaying, publishing or distributing any written material, visual images or sounds, which are threatening in nature and intended to stir up hatred against a group of people who are defined by reference to religious belief (or lack of religious belief) or sexual orientation.

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

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

Alder Grange restricts usage as follows:

9. User Restrictions

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	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					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	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				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X			
On-line gaming (non-educational)			X			
On-line gambling					X	
On-line shopping / commerce					X	
File sharing				X		
Use of social media					X	
Use of messaging apps					X	

Use of video broadcasting e.g. YouTube				X		

10. School Actions & Sanctions

It is more likely that Alder Grange will need to deal with any incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

	Actions / Sanctions								
Pupils Incidents	Refer to class teacher / tutor	Refer to Head of Department / Year / other	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			X	X	X	X	X		X
Unauthorised use of non-educational sites during lessons	X								
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X	X							
Unauthorised / inappropriate use of social media / messaging apps / personal email		X		X		X		X	X
Unauthorised downloading or uploading of files		X		X		X	X	X	X
Allowing others to access school / academy network by sharing username and passwords							X		X
Attempting to access or accessing the school / academy network, using another student's / pupil's account							X		X
Attempting to access or accessing the school / academy network, using the account of a member of staff		X		X		X	X	X	X
Corrupting or destroying the data of other users		X				X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X				X	X	X	X
Continued infringements of the above, following previous warnings or sanctions		X		X		X	X	X	X
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school		X	X			X	X	X	X
Using proxy sites or other means to subvert the school's / academy's filtering system					X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident					X			X	
Deliberately accessing or trying to access offensive or pornographic material		X		X	X	X	X	X	X

Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act					X	X	X	X	X

	Actions / Sanctions							
Staff Incidents	Refer to line manager	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X			X	X
Inappropriate personal use of the internet / social media / personal email		X	X	X		X		X
Unauthorised downloading or uploading of files		X	X	X		X		X
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X		X		X	X	X
Careless use of personal data e.g. holding or transferring data in an insecure manner						X		X
Deliberate actions to breach data protection or network security rules		X		X		X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X		X		X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X		X		X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X	X	X		X	X	X
Actions which could compromise the staff member's professional standing		X				X		X
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy		X				X		X
Using proxy sites or other means to subvert the school's / academy's filtering system		X				X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident		X				X		X
Deliberately accessing or trying to access offensive or pornographic material		X		X		X	X	X
Breaching copyright or licensing regulations	X					X		
Continued infringements of the above, following previous warnings or sanctions	X	X				X		X

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.

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.

.