Everyone matters, every day counts

E-SAFETY POLICY

Policy created: 05.01.15 Policy first adopted:

Signed chair of Governors:

Re-adopted & signed:

Consultation – E-safety working group: 12.11.15 SLT : 16.01.16

Staff Consultation: 11.01.16

TA Consultation: 19/01/16

E-SAFETY POLICY IMPLEMENTATION.

The e–Safety Policy and its implementation will be reviewed annually.

Our e–Safety Policy has been written by the college, building on government guidance.

Our College Policy has been agreed by the Senior Leadership Team and approved by governors and other stakeholders. All staff have been involved in the drafting of this policy and consulted about its contents.

The College e-Safety Coordinator is James Winchester, Interim Assistant Headteacher

Contents **Page**

Introduction

Oak Grove College sees the area of e-safety as an important life skill for our students as well in addition to a child protection issue and not one that is solely evident in ICT. All staff and pupils have a duty to be aware of their own and others' e-safety at all times.

At Oak Grove College we recognise that students will have different access and understanding of e-safety and the policy will be applied appropriately to the needs of the students.

1. **Scope**

2.1. This policy applies to Oak Grove College governing body, all teaching and other staff, whether employed by the County Council or employed directly by the college, external contractors providing services on behalf of the college, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the college. These individuals are collectively referred to as 'staff members' in this policy.

2.2. e-safety is not limited to college premises, college equipment or the college day, neither is it limited to equipment owned by the college. Any incident that happens during the college day will be reported in line with the flowchart for recording and reporting e-safety incidents.

2.3 Incidents from outside college that are disclosed or observed by staff will be dealt with in line with child protection/behaviour procedures and the procedures outlined in this policy.

2.4 e-safety concerns the day to day running of the physical network and information passing through it whether connected via the internet, virtual private networks, intranets or local area networks

2.5 Students are to be taught safe practices and that the e-safety policy will be monitored and enforced.

2.6 The college will respond to e-safety incidents involving members of the college (staff or students) as if they occurred during the college day, on the college site even if perpetrated using equipment not owned or operated by the college.

2. **Legal Framework**

3.1 Many young people, and indeed some staff, use the Internet regularly without being aware that some of the activities they take part in are potentially illegal.

3.2 The law is developing rapidly and changes occur frequently. Please note this section is designed to inform users of legal issues relevant to the use of communications, it is not professional advice.

3.3 Full details of the legal framework may be found in Appendix E

- Racial and Religious Hatred Act 2006
- Criminal Justice Act 2003
- Sexual Offences Act 2003
- Communications Act 2003 (section 127)
- Data Protection Act 1998
- The Computer Misuse Act 1990 (sections 1 — 3)
- Malicious Communications Act 1988 (section 1)
- Copyright, Design and Patents Act 1988
- Public Order Act 1986 (sections 17 — 29)
- Obscene Publications Act 1959 and 1964
- Protection from Harassment Act 1997
- Regulation of Investigatory Powers Act 2000
- Criminal Justice and Immigration Act 2008
- Education and Inspections Act 2006

3. Related Policies

4.1 This policy should be read in conjunction with the acceptable usage policy, child protection policy, anti-bullying policy, school technical security policy, behaviour management policy, staff handbook and in line with the flowchart for recording and reporting e-safety incidents.

4. Statement of duty of care

5.1 The designated person for child protection will have overall responsibility for all e-safety matters and will be informed of all incidents in line with the flowchart for recording and reporting e-safety incidents.

5.2 This said all staff have a responsibility to support e-safe practices in schools.

5.3 Students and staff at all levels need to understand their responsibilities and liabilities in the event of deliberate attempts to breach e-safety protocols or those laid out in the acceptable usage policy.

5. Teaching safe practices

6.1 All staff will be trained in good e-safety practices through the college's professional development activities including those given by internal and external trainers. All staff should complete Think U Know (TUK) training and in the event of new staff joining they will receive TUK training within their induction period.

6.2 Governors will have an overview of e-safety practice as an agenda item on an annual basis and will be updated as the policy is revised.

6.3 Students are taught e-safe practices throughout the college year, in line with the computing/PD curriculum, and teachers ensure that they respond to the needs of their class as and when e-safety discussions arise.

6.4 Students new to the college or those who may not have completed the previous year's e-safety training will receive updates from their class teacher to bring them in line with other pupils.

6. Statement of provision of safe environment in college (including monitoring of the policy)

7.1 The college currently provides access to the internet through Surfprotect as a filtered internet service provider (Exa-Networks). The college ensures that all hardware owned by the college network is provided with sufficient anti-virus and firewall protection.

7.2 Computer usage is monitored through the use of Impero. This has a built in keyword detector which will flag up any inappropriate words whilst staff and students are using the computers.

7.2 It is expected that all staff and pupils adhere to this policy at all times; it should be read in conjunction with the acceptable usage policy. The policy is monitored by both the Lead Practitioner and the Headteacher through the use of regular review with members of the college and in line with the flow chart for e-safety incidents.

8. Procedures to be followed in the event of a breach of e-safety

8.1 All instances of e-safety, whether by direct observation or disclosure, will be taken seriously.

8.2 The process to follow should an observation or disclosure be made is laid out clearly in the flow chart for e-safety incidents. The flow chart should be followed and incident report completed at the earliest opportunity and in any case within 24 hours.

8.3 The incident flow chart for e-safety incidents includes the protection of evidence should there be a serious breach of e-safety.

8.4 Serious is defined as any breach that is intentional, whether by a member of the school or aimed towards a member of the school. Any device that has been involved in a serious breach should be taken, if safe to do so, and placed within the locked server room for investigation.

8.5 All breaches whether serious or not will be recorded in line with the flow chart for e-safety incidents (appendix A). E-safety violations are saved on the Central Resource Library and logged in the Impero system.

8.6 E-safety incidents that are deemed as serious could be incidents of sexual or violent imagery, bullying, racist or offensive text, physical attack, e-attack or sexual grooming. In these cases the e-safety policy should be read with other appropriate policies such as Child Protection, Acceptable Use and Disciplinary. This may involve other agencies including police, social services and LSCB.

9. The physical environment Wireless networks

9.1 The school uses wireless networking; all wireless networks will be encrypted to WPA 2 standard.

9.2 During the installation of such networks all subcontractors installing Wireless Access Points would need to demonstrate that the required encryption is in place prior to them leaving the school site and the work being signed off as complete.

10. Password policy

10.1 The school operates an enforced password policy on network devices.

10.2 All network users agree that they will not attempt to access the school network using any other username/password than their own. This is in line with the Acceptable Use Policy.

11. Data transfer

11.1 Only sensitive data that is essential for staff to work on at home should be taken off site.

11.2 Class lists with tracking data may be taken off site, however pupil information taken from SIMS including home addresses, medical, educational and personal information should not be taken off site unless pre-arranged and agreed with the headteacher and only then should be removed in exceptional circumstances.

11.3 Any data that is removed from the school site should be removed on a school laptop with the normal level of e-safety security as outlined in this policy or on a hardware encrypted memory stick provided by the school. These are the only methods that sensitive data should be transferred.

11.4 Information regarding staff and pupils that needs to be shared between job-share staff and between teaching, support and administrative staff should be placed on the school network where usual data protection and e-safety measures are in effect.

11.5 Hardware encrypted USB memory sticks will be provided to staff should there be a requirement for them to do this and the encryption keys for such will be provided to staff to remember. These keys should not be written down.

11.6 All staff have a duty to ensure that non-school staff do not have access to school data being used at home as outlined in the Acceptable Use policy.

12. Staff bringing in files from home for Teaching and Learning.

12.1 Any member of staff that brings files from home for Teaching and Learning is responsible for ensuring that the file they propose to use in school is free from virus/spyware/malware and it is their responsibility to ensure that the material contained in the file is fit for purpose and does not contain any offensive or copyright material.

13. Monitoring and reporting procedures

13.1 Records of all incidents involving e-safety will be logged through the Impero Management Console and are also recorded on SIMS.

13.2 These records may be shared with legitimate agencies as necessary to ensure e-safety.

Policy Statements

14. Education – students

14.1 Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision.

14.2 e-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum is provided as part of the Computing/PD curriculum and is regularly reviewed.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Students should be taught in all lesson to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.

- Students should be taught to acknowledge the source of information used and to respect copyright when using material access on the internet.
- Students should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should 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 students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should 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 (eg 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.

15. Education – Staff

15.1 It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The e-safety Officer will provide advice/guidance/training to individuals as required.

16. Education – Parents

16.1 Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may

underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, VLE
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications

17. Technical – Infrastructure / equipment, filtering and monitoring

17.1 The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities.

17.2 For more details please refer to the Technical Security Policy

18. Personal Devices

18.1 The use of mobile phones and other personal devices by students and staff in college will be decided by the college and covered in the college Acceptable Use policy. College students should not have their mobile phones on them during the college day (exception for 6th Form students in social times).

18.2 The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the college community and any breaches will be dealt with as part of the college discipline/behaviour policy.

18.3. College staff may confiscate a phone or device if they believe it is being used to contravene the college's behaviour or bullying policy. The phone or device might be searched by the Senior Leadership Team with the consent of the pupil or parent/carer.

18.4 If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.

18.5 Mobile phones will not be used during lessons or formal college time unless as part of an approved and directed curriculum based activity with consent from a member of staff.

18.6 Electronic devices of all kinds that are brought in to college are the responsibility of the user. The college accepts no responsibility for the loss, theft or damage of such items. Nor will the college accept responsibility for any adverse health effects caused by any such devices either potential or actual.

19. Pupils' Use of Personal Device

19. 1 If a pupil breaches the college policy then the phone or device will be confiscated and will be held in a secure place in the relevant Pastoral Leader's Office. Mobile phones and devices will be released to parents/carers.

19.2 Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

19.3 If a pupil needs to contact his/her parents/carers they will be allowed to use a college phone. Parents are advised not to contact their child via their mobile phones during the college day, but to contact College Reception.

19.4 Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

20 Staff Use of Personal Devices

20.1 Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.

20.2 Mobile phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.

20.3 If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.

20.4 Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.

20.5 If a member of staff breaches the college policy then disciplinary action may be taken.

21. Use of digital and video images

21.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students 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.

21.2 The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students 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 eg on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website.
- Student's work can only be published with the permission of the student and parents or carers.

22. Data Protection

22.1 Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 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.

22.2 The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". (see Privacy Notice section in the appendix)
- It has a Data Protection Policy

- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed - Phillip Potter, Headteacher
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

22.3 Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- 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 data using encryption and secure password protected devices.

22.4 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 (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software

- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

23. Communications

23.1 A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

Communication Technologies	Staff and other adults				Students/Pupils			
	Allowed	Allowed at certain Times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobiles phones may be brought to school	X				X			
Use of mobile phones in lessons – Personal Use		X						X
Use of mobile phones in social time		X					X	
Taking photos on mobile phones				X				X
Use of other mobile devices for T&L eg. Tablets, gaming devices	X						X	
Use of personal email addresses on school network				X				X
Use of school email for personal email				X				X
Use of messaging apps		X				X		
Use of social media		X				X		
Use of blogs		X				X		

Student phones must be given in to the pastoral leads in the morning and locked away.

Student phones may be used for travel training. Staff should be using phones

6TH Form students are allowed to use phones at break times but must do this up in the 6th Form hub.

Use in specific lessons e.g. ICT/PD lessons

23.2 When using communication technologies, the 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 students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school, 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 or parents / carers (email, chat, 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.
- Students will be provided with email addresses for educational use.
- Students will be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be 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.

24. Social Media - Protecting Professional Identity

24.1 All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

24.2 The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

24.3 School staff should ensure that:

- No references should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

24.4 The school's use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

25. Unsuitable / Inappropriate activities

25.1 The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

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	
	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					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
On-line gaming (educational)		X				

On-line gaming (non educational)		X			
On-line gambling				X	
On-line shopping / commerce			X		
File sharing – use of cloud based storage only approved by the DFE	X				
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting eg Youtube			X		

25.2 The use of internet shopping and banking is acceptable for nominated users. Staff should be aware that this is for their own protection from loss of confidential information due to the monitoring systems in place (Impero software). Other users could potentially see this information when using this software.

26. Responding to incidents of misuse

26.1. This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above)

26.2 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 (appendix A) for responding to online safety incidents and report immediately to the police.

26. 3 Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of 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 a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group 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 national / local 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
    - other criminal conduct, activity or materials
    - Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child

27. School Actions and Sanctions

27.1. It is more likely that the school will need to deal with 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:

Students Actions/Sanctions

Incidents	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / othe	Refer to Headteacher / Senior Leader	Refer to Police	Refer to technical support staff for actionfre filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg 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	X	X	X
Unauthorised use of non-educational sites during lessons	X	X						X	
Unauthorised use of mobile phone / digital camera / other mobile device	X	X						X	X

Unauthorised use of social media / messaging apps / 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	X	X			X		X	X	
Attempting to access or accessing the school network, using another student's / pupil's account	X	X	X		X	X	X	X	X
Attempting to access or accessing the school 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	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		X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X		X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X					X	
Using proxy sites or other means to subvert the school's filtering system		X	X		X		X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X		X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	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	

Staff Action/Sanctions

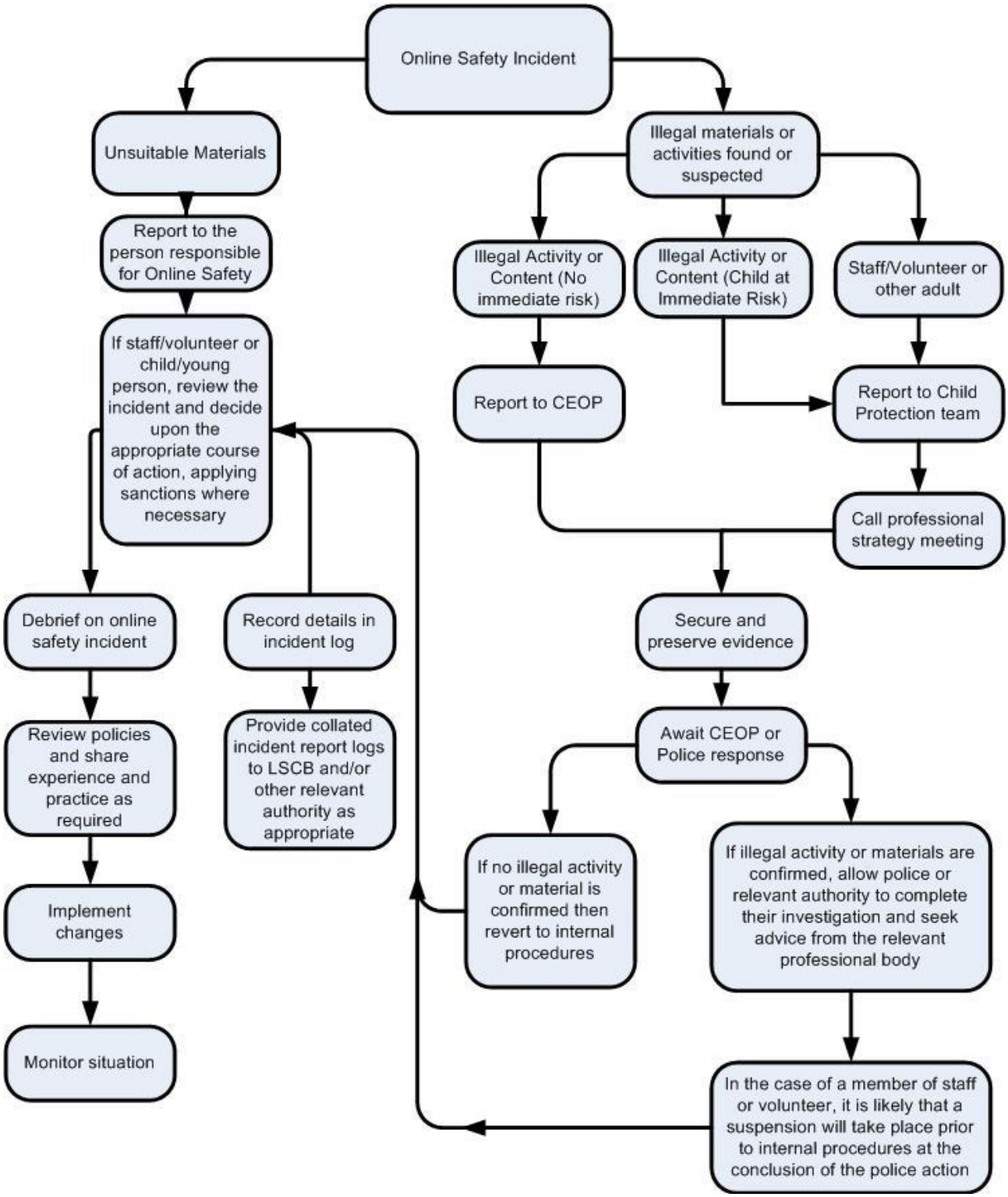
Incidents	Refer to line managerr	Refer to Headteacher/Senior Leader	Refer to Local Authority / HR	Refer to Police	Refer to technical support staff for action re filtering / security etc	Warning	Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X	X		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		
Careless use of personal data eg holding or transferring data in an insecure manner	X	X				X	
Deliberate actions to breach data protection or network security rules	X	X	X		X	X	X

There are student and teacher logins available for cover staff.

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 at any time		X	X	X			X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with **students / pupils under 18 or still in Education**		X	X			X	X
Actions which could compromise the staff member's professional standing	X	X	X			X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X		X	X	
Using proxy sites or other means to subvert the school's filtering system		X	X		X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X				X	X	
Breaching copyright or licensing regulations	X	X	X			X	X
Deliberately accessing or trying to access offensive or pornographic material		X	X	X		X	X
Continued infringements of the above, following previous warnings or sanctions		X	X	X		X	X

Appendices

Appendix A - Flowchart of how to respond to incidents



Appendix B – Privacy Notice

PRIVACY NOTICE for the school workforce employed or otherwise engaged to work at a school or the Local Authority

Privacy Notice - Data Protection Act 1998

Oak Grove College are the Data Controller for the purposes of the Data Protection Act.

Personal data is held by the school about those employed or otherwise engaged to work at the school. This is to assist in the smooth running of the school and/or enable individuals to be paid. The collection of this information will benefit both national and local users by:

- Improving the management of school workforce data across the sector;
- Enabling a comprehensive picture of the workforce and how it is deployed to be built up;
- Informing the development of recruitment and retention policies;
- Allowing better financial modeling and planning;
- Enabling ethnicity and disability monitoring; and
- Supporting the work of the School Teacher Review Body and the School Support Staff Negotiating Body.

This personal data includes some or all of the following - identifiers such as name and National Insurance Number and characteristics such as ethnic group; employment contract and remuneration details, qualifications and absence information.

We will not give information about you to anyone outside the school or Local Authority (LA) without your consent unless the law and our rules allow us to.

We are required by law to pass on some of this data to:

- the LA
- the Department for Education (DfE)

If you require more information about how the LA and/or DfE store and use this data please go to the following websites:

http://wsgfl.westsussex.gov.uk/ccm/content/leadership/education-research--information-unit/fair-processing-notices.en

and

http://www.teachernet.gov.uk/management/ims/datamanagement/privacynotices/workforcedata/

If you are unable to access these websites, please contact the LA or DfE as follows:

- Head of People Management
  Business Services
  West Sussex County Council
  Chichester

PO20 1RF

- Public Communications Unit
  Department for Education
  Sanctuary Buildings
  Great Smith Street
  London
  SW1P 3BT
  Website: www.education.gov.uk

  Email: info@education.gsi.gov.uk

  Telephone: 0870 000 2288.