LARKMEAD SCHOOL

E-SAFETY POLICY

Background

E-Safety exists to outline to young people the dangers related to their use of the internet. Some examples of this are:

- Bullying via chat or email
- Obsessive internet use
- Exposure to inappropriate materials including materials that seek to radicalise students and /or promote extremism
- Inappropriate or illegal behaviour
- Physical danger of sexual abuse

The purpose of the E-Safety policy is to:

- Keep students safe when using digital devices and technology both in and out of school
- Protect the school from any legal challenge relating to misuse of digital technology.
- Outline the actions that the school will take to ensure that students can work in an e-safe environment and that any e-safety issue is detected and dealt with in a timely and appropriate fashion.

The Policy

1. <u>The E-Safety Committee</u>

The School's E-Safety Committee consists of the Headteacher, Safeguarding officer; IT Network Manager; Business Manager; Head of ICT; one member of each of the Pastoral and Curriculum Group and an appointed governor.

2. <u>Monitoring, Review & Schedule</u>

Schedule for Development/Monitoring/Review

This e-safety policy was approved by the *Governing Body / Governors Sub Committee on:*	*Sep 16*
The implementation of this e-safety policy will be monitored by the:	*E-Safety committee*
Monitoring will take place at regular intervals:	*Termly*
Governing Body/Governors Sub Committee will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	*Annually at the first meeting of the Student Welfare Governor sub-committee in each academic year*
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new	

threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*September 2017*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*LADO – Alison Beasley*

3. Assessment of Impact of the Policy

The school will monitor the impact of the policy using:

- Logs of reported incidents
  - Cyberbullying/abuse based on data from bullying report system
  - Inappropriate materials based on safeguarding reports
  - Accessing of radical or extremist materials
- Scans of student work spaces
- Surveys / questionnaires of students, parents/carers and staff

4. To Whom does the Policy apply?

- All teaching and support staff
- All students
- All Governors & Parents
- All groups to sign appropriate 'Acceptable use policy'

This policy applies to all members of the school community (including staff, students, 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 Headteachers to such extent as is reasonable, to regulate the behaviour of students 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 e-safety incidents covered by this policy, which may take place outside of the school/academy, but is linked to membership of the school academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school 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 e-safety behaviour that take place out of school.)

5. Roles and responsibilities

A) Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors Student Welfare Committee Sub Committee receiving regular information about e-safety incidents and monitoring reports from the school. A member of the Governing Body has taken on the role of E-Safety Governor . The role of the E-Safety Governor will include making reports at each meeting of the Student welfare committee covering

- safety incidents

- Developments in e-safety e.g. the Prevent agenda
- E-Safety in the curriculum

B) Headteacher and Senior Leaders:

The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the e-Safety Co-ordinator/Officer.

The Headteacher and (at least) another member of the Senior Leadership Team, should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

C) E-Safety Officer/Safeguarding Lead

- leads the e-safety committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies & documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments

D) ICT Network Manager

The Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-safety technical requirements and any Local Authority E-Safety Policy/Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network/internet/Virtual Learning Environment/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/Senior Leader; E-Safety Officer for investigation, action or sanction as appropriate
- that monitoring software/systems are implemented and updated as agreed in school policies

- regular and random scans od students' workspace for inappropriate material/use

E) Teaching & Support Staff

Teaching & Support Staff will:

- have read, understood and signed the Staff Acceptable Use Policy
- report any suspected misuse or problem to the E-Safety Officer via the Safeguarding report form, for investigation, action or sanction as appropriate
- ensure all digital communications they have with students & parents/carers are on a professional level and only carried out using official school systems
- have an annual e-safety awareness update

Teachers will:

- When using the internet in lesson will make sure that students are properly briefed about what they should do if they are victims of cyberbullying/abuse; receive inappropriate materials
- Ensure that students understand it is not acceptable to try to access inappropriate materials or share the same with others
- Ensure that when students carry out research activities in their lessons they are aware of what both copyright and plagiarism mean
- Ensure that Students are directed to appropriate websites for the task they are undertaking
- 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.

F) Students:

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy
- should know how to carry out research tasks without breaching copyright and plagiarism
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will 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
- should understand the importance of adopting good e-safety practice to keep themselves safe when using digital technologies out of school and realise that the school's e-Safety Policy covers their actions out of school, if related to their membership of the school
- Should read and understand the school's 'E-Safety – Guidance to Students' document (at Appendix A to this policy)

G) Parents

Parents & Carers will:

- support the school e-Safety Policy by following good safety practice and guidelines. To assist in this is the school provides its ‘E-Safety – Guidance to Students’ document (at Appendix A to this policy)
- will be provided with support in dealing with e-Safety issues in and out of school where members of the school community are involved. Including the reporting of e-Safety and safeguarding concerns
-

6. E-Safety in the Curriculum

- E-Safety is module 1 to the Year 7 IT & computing curriculum, will be covered within the Personal Development Curriculum (PDC) and will be revisited throughout each key stage
- Key safety messages will be delivered through assemblies and/or special events
- Students should be taught in all lessons to be critically aware of the materials/ content they access on-line and be guided to validate the accuracy of information; they should also be aware of copyright and plagiarism
- 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 ICT Network Staff 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. A record of requests will be held by the ICT Network Manager

7. Training – Governors

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any subcommittee/group involved in technology/e-safety/health and safety or child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation
- Participation in school training / information sessions for staff or parents

8. Use of Personal Electronic Devices in School

Where personal electronic devices are permitted in school, their use must not contravene existing school policy and or safety policy. Guidance for the use of own devices is outlined below

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated

- Where possible these devices will be covered by the schools normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Students receive training and guidance on the use of personal devices

9. Use of Digital & Video Images

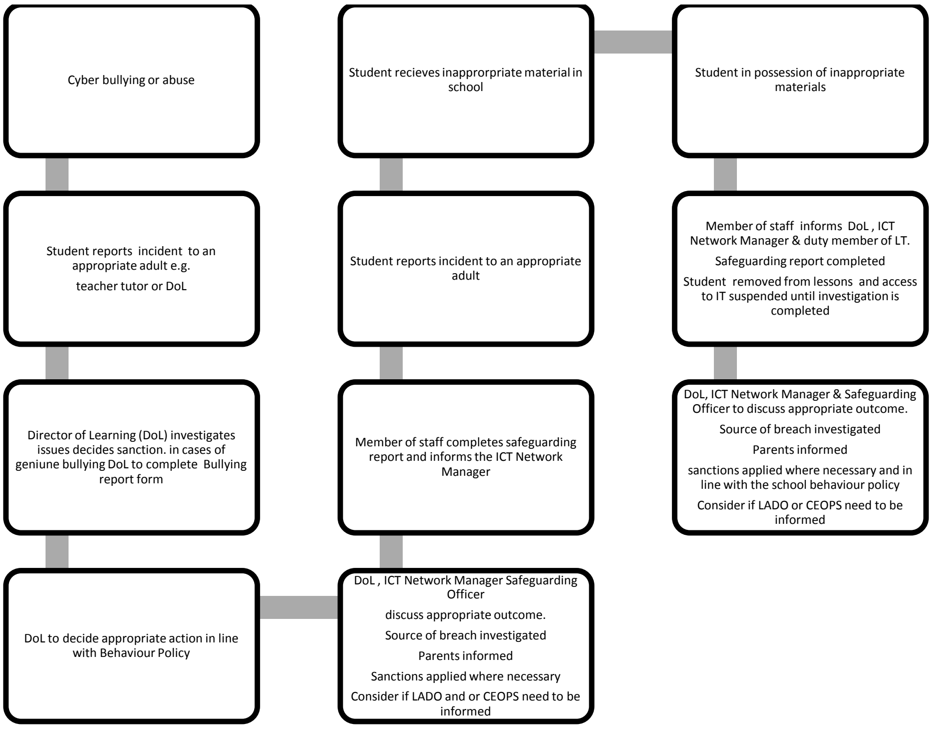
When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

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 or made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images.

Table to clarify what technical devices & media may be used in Larkmead School and by whom

	Staff & other adults				Students (KS 3&4)			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	•							•
Use of mobile phones in lessons		•						•
Use of mobile phones in social time	•							•
Taking photos on mobile phones		•						•
Taking photos on cameras		•					•	
Use of other mobile devices e.g. tablets		•					•	
Use of personal email addresses in school, or on school network				•				•
Use of school email for personal emails	•						•	
Use of messaging apps	•							•
Use of social media		•						•
Use of blogs		•						•

10. Responding to incidents of Cyber-bullying, Abuse & Misuse Student Report (either in school or out)



Cyber bullying or abuse

Student reports incident to an appropriate adult e.g.

teacher tutor or DoL

Director of Learning (DoL) investigates issues decides sanction. in cases of geniune bullying DoL to complete Bullying report form

DoL to decide appropriate action in line with Behaviour Policy

Student recieves inapprorpriate material in school

Student reports incident to an appropriate adult

Member of staff completes safeguarding report and informs the ICT Network Manager

DoL , ICT Network Manager Safeguarding Officer

discuss appropriate outcome.

Source of breach investigated

Parents informed

Sanctions applied where necessary

Consider if LADO and or CEOPS need to be informed

Student in possession of inappropriate materials

Member of staff informs DoL , ICT Network Manager & duty member of LT.

Safeguarding report completed

Student removed from lessons and access to IT suspended until investigation is completed

DoL, ICT Network Manager & Safeguarding Officer to discuss appropriate outcome.

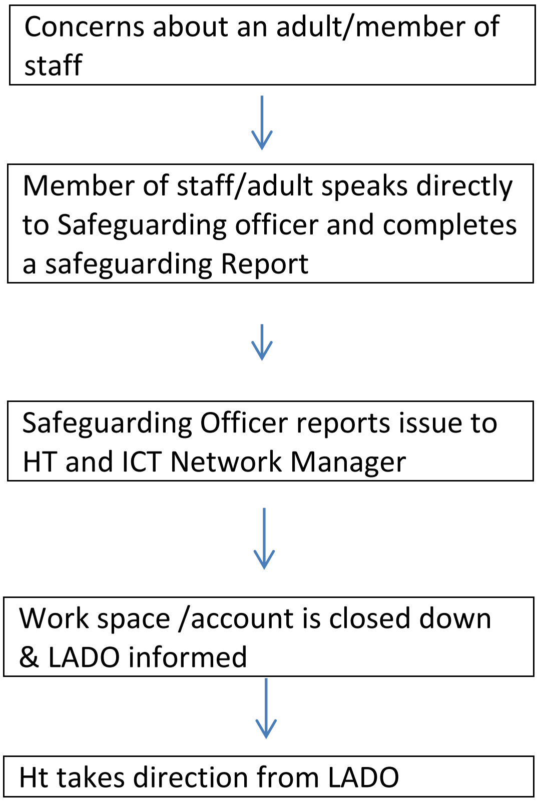
Source of breach investigated

Parents informed

sanctions applied where necessary and in line with the school behaviour policy

Consider if LADO or CEOPS need to be informed

Response to Concerns about a Member of Staff Misuse of Cyber Technology



Concerns about an adult/member of staff

Member of staff/adult speaks directly to Safeguarding officer and completes a safeguarding Report

Safeguarding Officer reports issue to HT and ICT Network Manager

Work space /account is closed down & LADO informed

Ht takes direction from LADO

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 / volunteer 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 protection purposes. The completed form should be retained by the group for evidence and reference purposes.

11. Data Protection

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

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".
- It has a Data Protection Policy It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)

12. School Actions & Sanctions

The school will take appropriate action where it is found that either a student or member of staff has contravened school policy.

Appendices:

A. Larkmead School E-Safety – Guidance to Students.

Appendix A to E-Safety Policy

E-Safety Guidance for Students

What is e-Safety?

What you should do if you are being abused (cyberbullied) via text, email and or social media in or out of school

- Save the texts, emails or other evidence
- **Do not** respond to the messages and **do not** confront the 'bully'. Remember they want a reaction from you, so please don't give them the satisfaction
- Tell and adult you trust about what is going on, they will help stop the abuse.
- If you would like more help or information about cyberbullying visit www.cybermentors.org.uk

What you should do if you suspect that someone else is a victim of abuse (cyberbullying) via text email or social media?

- **Tell them to** save the texts, emails or other evidence
- Tell them not to respond but to tell an adult they trust about what is going on.
- If they don't want to tell, you can do it on their behalf

What you should do if someone sends you inappropriate material or asks you to do something illegal or inappropriate via your phone or computer

- Make sure you keep the evidence. Don't respond, but don't unfriend them either
- Report the matter to an adult you trust straight away

Remember that:

Having and/or sending inappropriate images of someone under the age of 18 is illegal – this includes images of your self

It is unacceptable and often illegal, whether at home or in school, to try and access websites that contain inappropriate material

Some advice about keeping yourself safe on line

- **Set your privacy settings to private and check them from to time to time**
- **Check what is on your profile and think about the information it gives away about you. Does it make it easy for strangers to find out where you live or go to school?**
- **When you upload photos think about if you would be happy to show them to a stranger, your mum or even a future employer. It is very easy to lose control of information once it goes on the internet**
- **Remember if you chat on line the people you chat to may not always be telling the truth about themselves and who they are**
- **Never agree to meet a stranger that you met on line without an adult supervision.**
- **Add the ClickCEOP app to your Facebook file - www.facebook.com/clickceop**