Larkrise School & Wiltshire Learning Trust Online Safety Policy 2018

Includes the Responsible User Policy (RUP), Portable Devices Policy, Laptop Policy and Password Policy

1. Leadership and Management

1.1 Developing a policy

The school online policy features as part of the review process within the School Development Plan. It should relate to other policies for example behaviour, anti-bullying, personal, social and health education (PSHE), child protection and Staff Code of Conduct for Safer Working Practice.

- *Our online policy has been written by the school, building on the Wiltshire online template policy and government guidance. It has been agreed by the senior management and approved by governors. It will be reviewed annually.*

Created by:

Mary Seaman (Teacher/ICT Co-Ordinator)

Lynne Davies (ICT HLTA)

Mandy Cole (SBM)

Paul Gane (Named E-safety Governor)

Date: February 2017

Approved:

Review Date: May 2019

1.2 Authorised Access

Internet access for pupils should be seen as an entitlement on the basis of educational need and an essential resource for staff.

- *The school receives Internet Service Provision (ISP) from South West Grid for Learning (SWGfL) and has a service which proactively monitors Internet usage for attempts to access illegal (child abuse and incitement for racial hatred) content and will notify the local police and Wiltshire Council in these instances.*
- *The school receives Internet Service Provision (ISP) from South West Grid for Learning (SWGFL) and will request monitoring reports from the ISP which will be regularly checked to identify any attempts to access illegal content and should notify the local police and Wiltshire Council in these instances.*
- *The school will monitor through the SWGFL and relevant supervision of all staff and pupils who are granted Internet access.*
- *Access to the Internet will be by adult demonstration with directly supervised access to specific, approved online materials wherever possible.*

1.3 Filtering and Monitoring

Despite careful design, filtering systems cannot be completely effective due to the speed of change of web content. Levels of access and supervision will vary according to the pupil's age and experience. Internet access must be appropriate for all members of the school community from the youngest pupil to staff.

- *The school will work in partnership with parents, Wiltshire Council, DFE and its ISP to ensure systems to protect pupils are reviewed and improved.*
- *If staff or pupils discover unsuitable sites, the URL (web address) and content must be reported to the Internet Service Provider via the ICT HLTA.*
- *Website logs will be regularly sampled and monitored by the ICT HLTA and reported to the head teacher.*
- *The School will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.*
- *The staff proxy allowing access outside of regular filtering is only available under supervision by teachers and HLTAs with a regularly changed password.*
- *Any material that the school believes is illegal or may place an individual at risk must be referred to the appropriate authorities i.e. Head teacher, LADO, Police, Internet Watch Foundation.*

1.4 Risk Assessment

As the quantity and breadth of the information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The school will address the issue that it is difficult to remove completely the risk that pupils might access unsuitable materials via the school system.

- *In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Wiltshire Council can accept liability for the material accessed, or any consequences of Internet access.*
- *Methods to identify, assess and minimise risks will be reviewed regularly.*
- *The head teacher will ensure that the Online Safety Policy is implemented and compliance with the policy monitored.*
- *The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.*

2. Teaching and Learning

2.1 The Curriculum

The Internet is an essential resource to support teaching and learning. The statutory curriculum requires pupils to be responsible, competent, confident and creative users of information and communication technology. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources, e-mail and mobile learning. Computer skills are vital to access life-long learning and employment; indeed ICT is now seen as an essential life-skill.

- *Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.*
- *The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, ensure wellbeing, to support the professional work of staff and to enhance the school's management information and business administration systems.*
- *Whilst Internet access is an entitlement, users will need to show a responsible and mature approach to its use or this privilege may be removed.*
- *The Internet is an essential part of everyday life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.*
- *Larkrise School acknowledges the vulnerable nature of the cohort and therefore students will only have access to the internet when a member of staff is present.*
- *Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.*

2.2 Enhancing Teaching and Learning

Benefits of using the Internet in education include:

- *Access to a variety of worldwide educational resources.*
- *Inclusion in the National Education Network which connects all UK schools.*
- *Educational and cultural exchanges between pupils worldwide.*
- *Vocational, social and leisure use in libraries, clubs and at home.*
- *Access to experts in many fields for pupils and staff.*
- *Professional development for staff through access to national developments.*
- *Educational materials and effective curriculum practice.*
- *Collaboration across networks of schools, support services and professional associations.*
- *Improved access to technical support including remote management of networks and automatic system updates.*
- *Access to learning wherever and whenever convenient.*

2.3 Evaluating Content

Information received via the web, e-mail or text message requires good information-handling and digital literacy skills. In particular it may be difficult to determine origin and accuracy, as the contextual clues may be missing or difficult to read. A whole curriculum approach may be required.

Ideally inappropriate material would not be visible to pupils using the web but this is not easy to achieve and cannot be guaranteed. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

- *Pupils will be encouraged to be critically aware of the materials they read and how to validate information before accepting its accuracy.*
- *Pupils will use age-appropriate tools to research Internet content.*
- *The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.*
- *If staff or pupils discover unsuitable site or content they consider to be inappropriate, the URL (address) and content should be reported to their ISP/SWGfL*
- *Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.*
- *Pupils will be taught to acknowledge the source of information used and to respect individuals and intellectual property when using Internet material in their own work.*

3. Communication and Content

3.1 Website Content

Publication of any information online should always be considered from a personal and school security viewpoint. Sensitive information will be published in the school handbook. All content added to the Larkrise School website will need to reflect the school's requirements for accuracy and good presentation.

- *The point of contact on the school website is the school address, school e-mail and telephone number. Staff or pupils' personal information will not be published.*
- *Written permission from individuals, parents or carers will be obtained before photographs of pupils are published on the school website. Photographs will be selected carefully and will not enable individuals to be clearly identified.*
- *Pupils' full names will not be used anywhere on the website, particularly in association with photographs.*
- *The nature of all items uploaded will not include content that allows the pupils to be identified, either individually or through aggregated pieces of information.*
- *The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.*
- *The website should comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.*

3.2 Learning Platforms

An effective learning platform (LP) or virtual learning environment (VLE) can offer schools a wide range of benefits to teachers, pupils and parents, as well as support for management and administration.

- *All users will be required to use an age appropriate password to access the relevant content of the LP which must not be shared with others.*
- *SLT and staff will regularly monitor the usage of the LP by pupils and staff in all areas, in particular message and communication tools and publishing facilities.*
- *Pupils/staff will be advised about acceptable conduct and use when using the LP.*
- *Only members of the current pupil, parent/carers and staff community will have access to the LP.*
- *All users will be mindful of individual and intellectual property and will upload only appropriate content to the LP.*
- *When a user leaves the school their account or rights to relevant content areas will be disabled or transferred to their new establishment.*

3.3 Managing e-mail

E-mail is an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects between schools. However, the use of e-mail requires appropriate safety measures.

- *Pupils may only use approved e-mail accounts on the school system.*
- *Pupils must immediately tell a responsible adult if they receive offensive e-mail.*
- *Staff must use official school provided email accounts for all professional communications.*
- *Pupils should use email in an acceptable way. Sending images without consent, explicit images, messages that cause distress and harassment to others are considered significant breaches of school RUP and will be dealt with accordingly.*
- *E-mail sent to an external organisation should be written carefully and where appropriate, authorised before sending, in the same way as a letter written on school headed paper.*

3.4 On-line communications and Social Media.

On-line communications, social networking and social media services may be filtered in school by their ISP but are likely to be accessible from home.

All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published. Larkrise School has a key role to teach young people about the importance of how to communicate safely and respectfully online, keeping personal information private.

- *Users will be taught about how to keep personal information safe when using online services. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.*
- *Users must not reveal personal details of themselves or others in online communication, including the tagging of photos or video, or to arrange to meet anyone.*
- *Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.*
- *Staff official blogs or wikis should be password protected and only operate with approval from the SLT.*
- *Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.*

- *Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.*
- *No member of the school community should publish specific and detailed private thoughts about the school, especially those that may be considered threatening, hurtful or defamatory.*
- *Parents wishing to photograph or video at an event should be made aware of the schools expectations and be required to comply with the schools RUP as a condition of permission to photograph or record.*
- *Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.*
- *Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Responsible Use Policy (Appendix A).*
- *In line with, 'Guidance for Safer Working Practice for Adults who Work with Children and Young People' it will not be considered appropriate for staff to engage in personal online communications with children and young people, parents or carers. Express care is also to be taken regarding the use of social networking sites.*

3.5 Mobile Devices (Including Bring You Own Device-BYOD)

Mobile devices refer to any device that provides access to the internet or internal network for example, tablet (Apple Android, Windows, and other operating systems) e-readers, mobile phone, iPad, iPod touch, digital cameras.

Mobile devices can be used to facilitate communication in a variety of ways with text, images, sound and internet accesses all common features. A policy which prohibits users from taking mobile devices to school could be considered to be unreasonable and unrealistic for schools to achieve. Due to the widespread use of mobile devices it is essential that schools take steps to ensure that these devices, both personally and school owned, are used responsibly.

Allowing the use of mobile devices is a school decision, and should be subject to the following key principles:

- All individuals are protected from inappropriate material, bullying and harassment
- Users have access to resources to support learning and teaching
- Teachers and HLTAs will be allocated laptops. They should sign the Larkrise School Portable Devices Policy (Appendix B)
- Users should be given clear boundaries on responsible and professional use

The following points, whilst not exhaustive, have been provided to support schools in creating effective policies.

- *Mobile devices that are brought in to school remain the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items.*
- *School staff authorised by the Head teacher may search pupils or their possessions, and confiscate any mobile device they believe is being used to contravene school policy, constitute a prohibited item, is considered harmful, or detrimental to school discipline. If it is suspected that the material contained on the mobile device relates to a criminal offence, the device will be handed over to the Police for investigation*.
- *Sending abusive or inappropriate messages or content is forbidden by any user within the school community.*
- *Mobile devices are not permitted to be used in certain areas or situations within the school site e.g. changing rooms or toilets, situations of emotional distress etc.*
- *Where staff may need to contact children, young people and their families within or outside of the setting in a professional capacity, they should only do so via an approved school account (e.g. e-mail, phone, social media) In exceptional circumstances there may be a need to use their own personal devices and account; this should be notified to a senior member of staff ASAP.*
- *Staff should be provided with school equipment for the taking of photos or videos of pupils linked to an educational intention.*
- *For the safeguarding of all involved, users are encouraged to connect all school mobile devices through the school wireless provision and service that allows the ability to filter any device that uses the school Internet connection, without having to configure the user's device. Users will only be permitted to connect their own devices to the guest school wireless provision (see RUP Appendix A).*
- *The school will take steps to monitor responsible use in accordance with the Responsible Use Policy (Appendix A).*

3.6 Video Conferencing

Video conferencing (including FaceTime, Skype and Lync) enables users to see and hear each other between different locations. This 'real time' interactive technology has many potential benefits in education and where possible should take place using the school's wireless system.

- *Staff must refer to any Responsible Use agreements prior to children taking part in video conferences.*
- *All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.*
- *Pupils will ask permission from a teacher before making or answering a video conference call.*
- *Video conferencing will be supervised appropriately for the pupil's age and ability.*

3.7 Emerging Technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment should be completed or safety established on each new technology and assessed for effective and safe practice in classroom use. The safest approach is to deny access until a risk assessment has been completed and safety has been established.

- *Emerging technologies will be examined for educational benefit and a risk assessment will be carried out or safety will be established before use in school is allowed.*

3.8 Cyber Bullying

Cyber bullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet, to deliberately hurt or upset someone" DCSF 2007.

For most, using the internet and mobile devices is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. It is essential that young people, school staff, parents and carers understand how cyber bullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

Cyber bullying (along with all other forms of bullying) of or by any member of the school community will not be tolerated. Full details are set out in the school's behaviour, **anti-bullying and child protection policies**, which include:

- *Clear procedures set out to investigate incidents or allegations of cyber bullying.*
- *Clear procedures in place to support anyone in the school community affected by cyber bullying.*
- *Child Protection forms should be used if an incident occurs.*
- *All incidents of cyber bullying reported to the school will be recorded.*
- *The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the ISP and the police, if necessary.*
- *Pupils, staff and parents/carers will be required to work with the school to support the approach to cyber bullying and the school's e-Safety ethos.*

3.9 Data Protection

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 1998 gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. On May 25th 2018 the GDPR (General Data Protection Regulation) will come into force.

For advice and guidance relating to a contravention of the Act, contact www.wiltshire.gov.uk

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

4 Implementation

4.1 Policy in Practice - Pupils

Many pupils are very familiar with Internet use and the culture that surrounds it. As part of the school's e-safety teaching and awareness-raising it is important to discuss the key features with pupils / students as appropriate for their age and cognitive ability. Pupils will need to be reminded of the school rules at the point of Internet use.

- *All users will be informed that network and Internet use will be monitored.*
- *Online Safety teaching should be integral to the curriculum and raise the awareness and importance of safe and responsible internet use amongst pupils.*
- *Online Safety teaching will be included in PSHE, Citizenship and/or Computing and cover safe use at school and home.*
- *Online Safety rules will be on display in all rooms with Internet access.*
- *Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.*

4.2 Policy in Practice - Staff

It is important that all staff feel confident to use new technologies in teaching and the School Online Safety Policy will only be effective if all staff subscribe to its values and methods. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies.

Particular consideration must be given when members of staff are provided with devices by the school which may be accessed outside the school network. Schools must be clear about the safe and appropriate uses of their school provided equipment and have rules in place about use of the equipment by third parties. Staff must be made aware of their responsibility to maintain confidentiality of school information. If a member of staff is concerned about any aspect of their ICT or internet use either on or off site, they should discuss this with their senior leader to avoid any possible misunderstanding.

- *The Online Safety Policy will be provided to and discussed with all members of staff and Responsible User Policy signed for compliance.*
- *Staff should be aware that Internet traffic is monitored (and automatically reported by the SWGfL) and can be traced to the individual user. Discretion and professional conduct is essential.*
- *Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.*
- *Staff should be aware that any breaches of the Online Safety Policy will be a disciplinary matter (see Disciplinary Policy).*
- *All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.*

4.3 Policy in Practice - Parents

Parents need to be aware of the potential dangers that are associated with online communications, social networking sites and mobile technologies to help ensure their children are not putting themselves at risk.
The school website has links to websites which can support online safety at home.

- *Parents' attention will be drawn to the Online Safety Policy and Responsible User Policy RUP (Appendix A) in newsletters, school prospectus, Website and the Home School Diaries.*
- *A partnership approach with parents will be encouraged. This could include offering parent evenings, demonstrations, practical sessions and suggestions for resources and safer Internet use at home.*
- *Regular information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home.*
- *Internet issues will be handled sensitively to inform parents without undue alarm.*
- *Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.*

4.4 Handling of complaints

Parents and teachers must know how and where to report incidents in line with the school complaints policy and complaints of a child protection nature must be dealt with in accordance with the LA Child Protection procedures. Prompt action will be required if a complaint is made. The facts of the case will need to be established; for instance whether the Internet use was within or outside school. A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's behaviour policy. All records of the incident should be kept, e.g. e-mails saved or printed, text messages saved etc.

- *Responsibility for handling incidents will be delegated to a senior member of staff.*
- *Any complaint about staff misuse must be referred to the head teacher.*
- *Pupils and parents will be informed of the complaints procedure.*
- *Parents and pupils will need to work in partnership with staff to resolve issues.*
- *There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.*

Appendix A
Larkrise School – Responsible User Policy (RUP)
(Supports Online Safety Policy) – May 2018

Larkrise School recognises the important contribution and value technology can play in promoting students' learning and development, however, there are potential risks involved. We have a rigorous online safety policy and procedures in place and have taken positive steps to reduce this risk in school as we believe that the benefits to students from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages.
Allowing the use of mobile devices is a school decision, and should be subject to the following key principles:

- All individuals are protected from inappropriate material, bullying and harassment
- Users have access to resources to support learning and teaching
- Users should be given clear boundaries on responsible and professional use

Access to network services is given to users who act in a considerate, appropriate and responsible manner. Users are responsible for their behaviour on school networks just as they are in any part of the school. Access is a privilege—not a right—and entails responsibility. We expect all users to use technology, both that belonging to the school or their own, responsibly and strictly according to the following conditions:
For the purposes of this document, technology means any device that provides a connection to the Internet or internal network.

1. A device loaned to you by the school for an education related purpose remains the property of Larkrise School.
2. Only approved user devices may connect to the school network by prior agreement. Users may connect to the guest wifi provision.
3. A device must remain in your possession, should only be used by you and should be securely stored when not in use.
4. Larkrise School policies regarding the appropriate use and sharing information apply to devices both school and privately owned. Use of any device must adhere to data protection, online safety and health and safety rules.
5. Devices may be used for education related purposes at the discretion and under the supervision of the teacher or responsible adult.
6. If used to create or store personal information including images and videos of pupils, users must fully comply with high standards of data protection as set out in the Data Protection Act 1998.
7. A device connecting to the school network may be configured with certain restrictions in place. Any settings that are password protected must not be changed.
8. Insurance cover provides protection for school owned devices from the standard risks whilst the device is on site or in your home **but excludes** theft from a car or other establishment. Should the device be left unattended and is stolen, you will be responsible for its replacement.
9. Privately owned devices remain the responsibility of the owner and will not be covered under the school insurance policy.
10. All devices whether owned by the school or privately owned, may be subject to regular checks for compliance with school policies. Failure to comply or evidence of unacceptable use will result in sanctions or disciplinary action.

Unacceptable use includes but is not limited to:

- Making, storing, posting, downloading, uploading or passing on, material, remarks or images that may be offensive or upsetting to an individual or group;
- Making, storing, posting, downloading, uploading or passing on images of individuals without their permission This includes taking photographic images of school pupils on personal phones, cameras, tablets or other devices;
- Giving personal information, such as complete name, phone number, address or identifiable photo, without permission from teacher and parent or guardian;
- Using obscene language;
- Damaging or modifying computers, computer systems or computer networks: downloading, installing and using games, audio files, video files or other applications including shareware or freeware without permission to do so;
- Violating copyright laws ;
- Sharing or using others' logons or passwords or other confidential information;
- Trespassing in others' folders, work or files;
- Intentionally wasting limited resources;
- Unreasonably leaving laptops, cameras, tablets, PCs and other devices unattended and vulnerable to breakage, damage or theft;
- Disregarding the importance, value and responsibility of laptops, cameras, tablets, PCs and other devices by not looking after them appropriately;
- Employing the network for non-academic, personal, commercial, political purposes, financial gain, or fraud;
- Attaching unauthorized equipment to the school network.

It is not acceptable to use personal phones or other devices in curriculum time (either in the classroom, playground and other curriculum periods). In emergencies or challenging periods where use of personal devices are essential seek formal permission from your Line Manager.

I have read this agreement and fully understand that I need to adhere to all elements. I understand that the Responsible User Policy is intended to safeguard all members of the Larkrise Community.

User signature: …… Date: ……

- ***Please take a photocopy of your signed RUP and return to the School Office (Carole Simpson)***
- ***You are reminded that you are always subjected to the Data Protection Act 1998, Computer Misuse Act 1990 and Copyright, Designs and Patents Act 1988.***

Appendix B
Larkrise Portable Devices Policy
May 2018

1. Laptops remain the property of Larkrise School.
2. A laptop is allocated to a named member of staff and is their responsibility. If another member of staff borrows it, the responsibility still stays with the teacher allocated. Only Larkrise School Staff should use the laptop. All staff must sign for their laptop. **See attached.**
3. On the teacher leaving the school's employment, the laptop is returned to Larkrise School. Staff on extended leave of 4 weeks and over should return their laptops to the school (other than by prior agreement with the headteacher).
4. Staff should take responsible steps to keep their laptop safe.
5. The laptop must not be taken abroad, other than as part of a school trip and its use agreed by prior arrangement with the headteacher with evidence of adequate insurance.
6. All software must be loaded onto school ICT equipment by the ICT/HLTA.
7. If any removable media is used then it must be checked to ensure it is free from any viruses.
8. It will be the responsibility of the member of staff to ensure virus protection software that has been installed on the laptop is kept up-to-date.
9. Staff should be mindful that regular access to the school network will ensure virus protection is automatically updated.
10. Staff should not attempt to significantly alter the computer settings other than to personalise their desktop working area.
11. Students must never use staff laptops with the exception of via smart boards or plasma screens.
12. If any fault occurs with the laptop, it should be referred immediately to the technician via the Apollo online request system or report to the ICT/HLTA.
13. When being transported, the carrying case or other protective carrier must be used at all times.
14. The laptop should be covered by normal household insurance. If not it should be kept in school and locked up overnight.

Policy for responsible e-mail, network and Internet use for Larkrise School

1. I will only access the system with my own name and registered password, which I will keep secret.
2. I will inform the Network Manager/School's Technician as soon as possible if I know my password is no longer secret.
3. I will always log off the system and 365 email when I have finished working.
4. My files should not, routinely, be password protected by my own passwords. Should a confidential matter warrant this, I must gain permission from the headteacher and register the passwords with the headteacher.
5. If I use removable media (e.g. memory stick) I should be mindful that this may risk the introduction of viruses to the school system.
6. I will not open e-mail attachments unless they come from a recognised and reputable source. I will bring any other attachments to the attention of the Network Manager.
7. All joke e-mails and attachments are potentially damaging and undesirable and therefore should not be used.

8. I will report immediately to the headteacher any unpleasant material or messages sent to me.
9. Use for personal financial gain, gambling, political purposes or advertising is forbidden.
10. Storage of e-mails and attachment should be kept to a minimum to avoid unnecessary drain on memory and capacity.
11. Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
12. I understand that if I do not adhere to these rules, my network access will be suspended immediately, my laptop removed and that other disciplinary consequences may follow.

Print Name: .....

Signature: .....

Position: .....

Date: .....

Please sign, take a photocopy and return to the School Office (Carole Simpson)

Please complete page 3 when issued with a laptop and return to the School Office also.

Larkrise School Laptop Policy
May 2018

Per item 2 of the Laptop Policy (all staff must sign for their laptop), please complete details below:-

Staff Name:- .....

Date laptop policy distributed:- .....

Make and Model of Laptop:- .....

.....

.....

Serial Number of Laptop:- .....

Comments:- .....

.....

.....

.....

Signed:- .....

Print Name:- .....

Date:- .....

Please return to the School Office (Carole Simpson)

Appendix C
School Password Policy

School Technical Security Policy Template (including filtering and passwords)

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the *school infrastructure / network* is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of Lynne Davies (ICT HLTA), Mary Seaman (Computing Lead), and the Senior Leadership team should have an overview.

Technical Security

Policy statements

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 will receive guidance and training and will be effective in carrying out their responsibilities:

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements**
- **There will be regular reviews and audits of the safety and security of school technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.**
- **Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff.**
- **All users will have clearly defined access rights to school technical systems.**

- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- *Mobile device security and management procedures are in place.*
- *Remote management tools are used by staff to control workstations and view users activity*
- *An appropriate system is in place for users to report any actual / potential technical incident to the ICT HLTA (or other relevant person).*
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school system.
- *An agreed policy is in place regarding the downloading of executable files and the installation of programmes on school devices by user (password protection).*
- *An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.*
- *An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices.*
- *The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.*
- *Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.*

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

Policy Statements

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Online safety Committee (or other group).
- **All school networks and systems will be protected by secure passwords that are regularly changed**
- **The "master / administrator" passwords for the school systems, used by the technical staff must also be available to the *Headteacher* or other nominated senior leader and kept in a secure place eg school safe.**
- *Passwords for new users, and replacement passwords for existing users will be allocated by the ICT HLTA or Apollo. Any changes carried out must be notified to the manager of the password security policy (above).*
- All users will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- *Users will change their passwords at regular intervals – as described in the staff and student / pupil sections below.*
- *Requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user.*

Staff passwords:

- **All staff users will be provided with a username and password** by *the ICT HLTA who will keep an up to date record of users and their usernames.*
- *the password should ideally be a minimum of 8 characters long and could include three of – uppercase character, lowercase character, number, special characters*
- *must not include proper names or any other personal information about the user that might be known by others*
- *temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on*
- *passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)*
- *passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school*
- should not be re-used for 6 months and be significantly different from previous passwords created by the same user.
- should be different for different accounts, to ensure that other systems are not put at risk if one is compromised
- should be different for systems used inside and outside of school

Student / pupil passwords

- **Some identified users will be provided with a username and password, if appropriate.**
- Students / pupils will be taught the importance of password security
- The complexity (ie minimum standards) will be set with regards to the cognitive ability of the children.

Training / Awareness

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's online safety policy and password security policy
- through the Acceptable Use Agreement

Pupils / students will be made aware of the school's password policy:

- in lessons.