Jesson’s CE Primary School (VA)

E-Safety Policy

Includes

Acceptable Use Policy

and

Password Policy

March 2021

Signed by:

________________________ Headteacher Date: ________________________

________________________ Chair of Governors Date: ________________________

Contents

Scope

This guidance applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

Development, Monitoring and Review of the E-Safety Policy:

This E-Safety policy has been developed by a working group/committee made up of:

- School E-Safety Coordinator
- Headteacher
- Governors
- ICT technical support staff

Consultation with the whole school community has taken place through the following:

- Staff meetings
- Governors meetings

The school will monitor the impact of the policy using**:**

- Logs of reported incidents
- DGfL or internal monitoring logs of internet activity (including sites visited)
- Internal monitoring of data for network activity
- Surveys/questionnaires of stakeholders

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the E-Safety Policy.

Headteacher and Senior Leaders:

The Headteacher is responsible for ensuring the safety (including E-Safety) of members of the school community and is the school's Senior Information Risk Owner (SIRO). The School's SIRO is responsible for reporting security incidents as outlined in the School's Information Security Policy. The day to day responsibility for E-Safety will be delegated to the E-Safety Co-ordinator who has this responsibility

- The Headteacher is responsible for ensuring that the E-Safety Coordinator and other relevant staff, receive suitable CPD to enable them to carry out their E-Safety roles and to train other colleagues, as relevant. They are also responsible for ensuring that pupils and students are taught how to use ICT tools such as the internet, email and social networking sites, safely and appropriately.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The SLT will receive monitoring reports from the E-Safety Co-ordinator.
- The Headteacher and another member of the SLT 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.
- The Headteacher is responsible for ensuring that parents and carers, when given access to data and information relating to their child/children via the learning platform, have adequate information and guidance relating to the safe and appropriate use of this on-line facility.

E-Safety Coordinator:

The School has a named person with the day to day responsibilities for E-Safety.

Responsibilities include:

- Taking day to day responsibility for E-Safety issues and having a leading role in establishing and reviewing the school E-Safety policies/documents
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
- Providing training and advice for staff
- Liaising with the Local Authority
- Liaising with the schools SIRO to ensure all school data and information is kept safe and secure
- Liaising with school ICT technical staff and/or school contact from the managed service provider- RM
- Receiving reports of E-Safety incidents and creating a log of incidents to inform future E- Safety developments
- Meeting regularly with the E-Safety Governor to discuss current issues, review incident logs and filtering.
- Attending relevant meetings/Governor committee meetings
- Reporting regularly to Senior Leadership Team

Managed service provider:

The managed service provider (RM) is responsible for helping the School to ensure that it meets the E-Safety technical requirements outlined by DGfL. The managed service provides a number of tools to schools including RmsafetyNet and eSafe, which are designed to help schools keep users safe when on-line in school-*(see appendix* 2). These will also monitor pupils who are using school Chromebook devices both inside and outside school.

Many of the settings are controlled at a local authority level, however the school can request changes to be made, if required.

Members of the DGfL team will support schools to improve their E-Safety strategy.

The managed service provider maintains backups of email traffic for 90 days. If access to this information is required, the school should contact the DGfL team.

Teaching and Support Staff:

Are responsible for ensuring that:

- They have an up to date awareness of E-Safety matters and of the current school E-Safety policy and practices
- They encourage pupils to develop good habits when using ICT to keep themselves safe
- They have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- They report any suspected misuse or problem to the E-Safety Co-ordinator/Headteacher/ Assistant Headteacher/class teacher for investigation/action/sanction.
- Digital communications with students/pupils (email/Virtual Learning Environment (VLE)/voice) should be on a professional level and only carried out using official school systems
- E-Safety issues are embedded in all aspects of the curriculum and other school activities
- Students/pupils understand and follow the school E-Safety and acceptable use policy.
- Students/pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons, extra-curricular and extended school activities
- They are aware of E-Safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices
- In lessons where internet use is pre-planned, students/pupils 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. They include the teaching of E-Safety in their lessons.

Designated person for Child Protection/Child Protection Officer:

The named person is trained in E-Safety issues and is aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Students/pupils:

Students/pupils have access to the school network and technologies that enable them to communicate with others beyond the school environment. The network is a secure and safe system provided through DGfL.

Students/pupils:

- Are responsible for using the school ICT systems in accordance with the Student/Pupil Acceptable Use Policy *(see appendix 3*), which they will be expected to sign before being given access to school systems.
- Need to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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 school policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on the taking/use of images, use of social networking sites and on cyber-bullying
- Should understand the importance of adopting good E-Safety practice 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 the use of an externally available web-based system, provided by the school

Parents/Carers:

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local E-Safety campaigns /literature.

Parents and carers will be responsible for:

- Endorsing (by signature) the Student/Pupil Acceptable Use Policy
- Accessing the school website/Learning Platform/in accordance with the relevant school Acceptable Use Policy.

Community Users/'Guest Access':

Community Users who access school ICT systems/website/VLE as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems- see appendix 3.

Education – students/pupils

There is a planned and progressive E-Safety curriculum. Learning opportunities are embedded into the curriculum throughout the school and are taught in all year groups.
E-Safety education is provided in the following ways:

- A planned E-Safety/E-literacy programme is provided as part of ICT and is regularly revisited – this include the use of ICT and new technologies in school and outside school
- Students/pupils are 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
- Students/pupils are aware of the Student AUP and are encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Students/pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students and pupils are taught the importance of information security and the need to keep information such as their password safe and secure
- Staff act as good role models in their use of ICT, the internet and mobile devices

Education – parents/carers

The school provides information and awareness to parents and carers through:

- Letters, newsletters, web site
- Parents evenings

Education & Training – Staff

All staff receive regular E-Safety training and understand their responsibilities, as outlined in this policy. Training is offered as follows:

- A planned programme of formal E-Safety training is made available to staff. An audit of the E-Safety training needs of all staff is carried out regularly. It is expected that some staff will identify E-Safety as a training need within the performance management process
- All new staff receive E-Safety training as part of their induction programme, ensuring that they fully understand the school E-Safety Policy and Acceptable Use Policies
- The E-Safety Coordinator (or other nominated person) receives regular updates through attendance at training sessions and by reviewing guidance documents released by DfE/DGfL/LA and others.
- This E-Safety policy and its updates are presented to and discussed by staff in staff/team meetings / INSET days
- The E-Safety Coordinator provides advice/guidance/training as required to individuals

All staff are familiar with the schools' Policy including:

- Safe use of e-mail
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network
- Safe use of school network, equipment and data
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras
- Publication of pupil information/photographs and use of website
- Cyber bullying procedures

- Their role in providing E-Safety education for pupils
- The need to keep personal information secure

Technical – infrastructure/equipment, filtering and monitoring

The managed service provider is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible. The school is responsible for ensuring that policies and procedures approved within this policy are implemented.

School ICT systems will be managed in ways that ensure that the school meets the E-Safety technical requirements outlined in the Acceptable Use Policies

- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems
- All users will be provided with a username and password
- Users will be made responsible for the security of their username and password. They 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
- The school maintains and supports the managed filtering service provided by DGfL
- The school can provide enhanced user-level filtering through the use of RM SafetyNet
- The school manages and updates filtering issues through the RM helpdesk
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager/ICT Coordinator. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee.
- 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 E-Safety incident to the relevant person
- The managed service provider ensures that appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data
- An agreed procedure is in place for the provision of temporary access to “guests” (eg trainee teachers, visitors) onto the school system
- An agreed procedure is in place regarding the downloading of executable files by users
- The school infrastructure and individual workstations are protected by up to date virus software
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured

Curriculum

E-Safety is a focus in all areas of the curriculum and staff re-enforce E-Safety messages in the use of ICT across the curriculum.

- In lessons, where internet use is pre-planned, students/pupils are guided to sites checked as suitable for their use and there are processes in place for dealing with any unsuitable material that is found in internet searches- using the search engine ICE. Children's use of other unfiltered search engines such as Google/Bing etc is not permitted.
- Where students/pupils are allowed to freely search the internet, e.g. using search engines, staff should monitor the content of the websites the young people visit
- The school provides opportunities within a range of curriculum areas to teach about E-Safety
- 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 Network Manager or managed service provider temporarily remove those sites from the filtered list for the period of study. Any requests to do so are auditable and should be logged
- Students/pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information
- Students/pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies, i.e. parent/carer, teacher/trusted staff member, or an organisation such as Childline or CEOP report abuse button.

Use of digital and video images

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

- Staff are allowed to take digital/video images to support educational aims, and follow school policies concerning the sharing, distribution, and publication of those images. Those images are only taken on school equipment, the personal equipment of staff (e.g. mobile phones, personally owned iPads) are not used for such purposes
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips.
- Care is taken when capturing digital/video images, ensuring students/pupils are appropriately dressed and that they are not participating in activities that might bring the individuals or the school into disrepute
- Students/pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and comply with good practice guidance on the use of such images
- Students/pupils full names will not be used anywhere on a website or blog, particularly in association with photographs if a parent has informed the school in writing they do not give their permission for this

Data Protection

Please refer to the separate Data Protection Policy.

Communications

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. Staff and students/pupils should therefore use only the school email service to communicate with others when in school, or on school systems e.g. by remote access from home
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and students/pupils 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 public chat / social networking programmes must not be used for these communications
- Students/pupils are provided with individual school email addresses for educational use (as deemed appropriate)
- Students/pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff
- Mobile phones may not be brought into school by pupils/students
- If pupils do bring personal mobile devices/phones to school they must not use them for personal purposes within school time. At the beginning of the day the device should be labelled and stored in the school safe/office until it is collected by an adult/pupil at the end of the day. At all times the device must be switched off or onto silent
- The school allows staff to bring in personal mobile phones and devices for their own use, but these should be used in accordance with the staff code of conduct.
- Under no circumstances should a member of staff contact a pupil or parent/ carer using their personal device unless authorised to do so by the school.
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device
- The School provides a safe and secure way of using chat rooms, blogs and other 'social networking technologies' via the Learning Platform. No other 'social networking' sites are permitted to be used in school, these will be blocked by RM SafetyNet when using a school computer.

Unsuitable/inappropriate activities

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

The school will take all reasonable precautions to ensure E-Safety.

However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview/counselling by teacher/Assistant Headteacher/E-Safety Coordinator/ Headteacher
- Informing parents or carers.
- Removal of Internet or computer access for a period, (which could ultimately prevent access to files held on the system, including examination coursework).
- Referral to LA/Police.

The LA has set out the reporting procedure for E-Safety incidents (see Appendix 1).

Our E-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.
- Complaints related to child protection are dealt with in accordance with school/LA child protection procedures

There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

Date the Policy was approved by Governors ……………………………….

Date for review

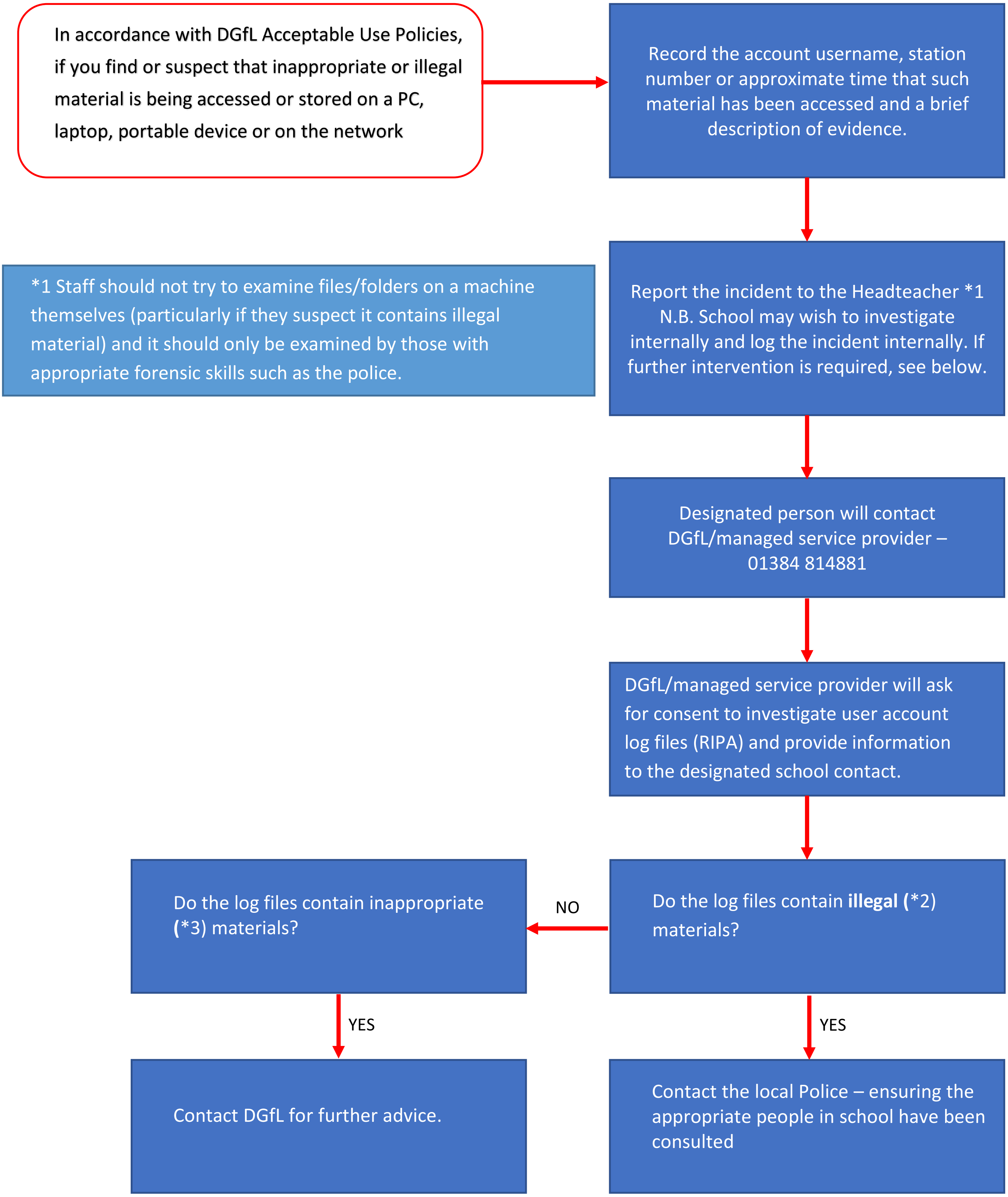
………………………………….. Contact

…………………………………..

This E-Safety Guidance and Policy has been written with references to the following sources of information:

BECTA
Dudley
LA
Hertfordshire E-Safety Policy
Kent e-Safety Policies, Information and Guidance
South West Grid for Learning- School E-Safety Policy

Guidance procedure for E-Safety incidents -Staff user incidents



In accordance with DGfL Acceptable Use Policies, if you find or suspect that inappropriate or illegal material is being accessed or stored on a PC, laptop, portable device or on the network

Record the account username, station number or approximate time that such material has been accessed and a brief description of evidence.

Report the incident to the Headteacher *1 N.B. School may wish to investigate internally and log the incident internally. If further intervention is required, see below.

*1 Staff should not try to examine files/folders on a machine themselves (particularly if they suspect it contains illegal material) and it should only be examined by those with appropriate forensic skills such as the police.

Designated person will contact DGfL/managed service provider – 01384 814881

DGfL/managed service provider will ask for consent to investigate user account log files (RIPA) and provide information to the designated school contact.

Do the log files contain **illegal** (*2) materials?

YES

Contact the local Police – ensuring the appropriate people in school have been consulted

NO

Do the log files contain inappropriate (*3) materials?

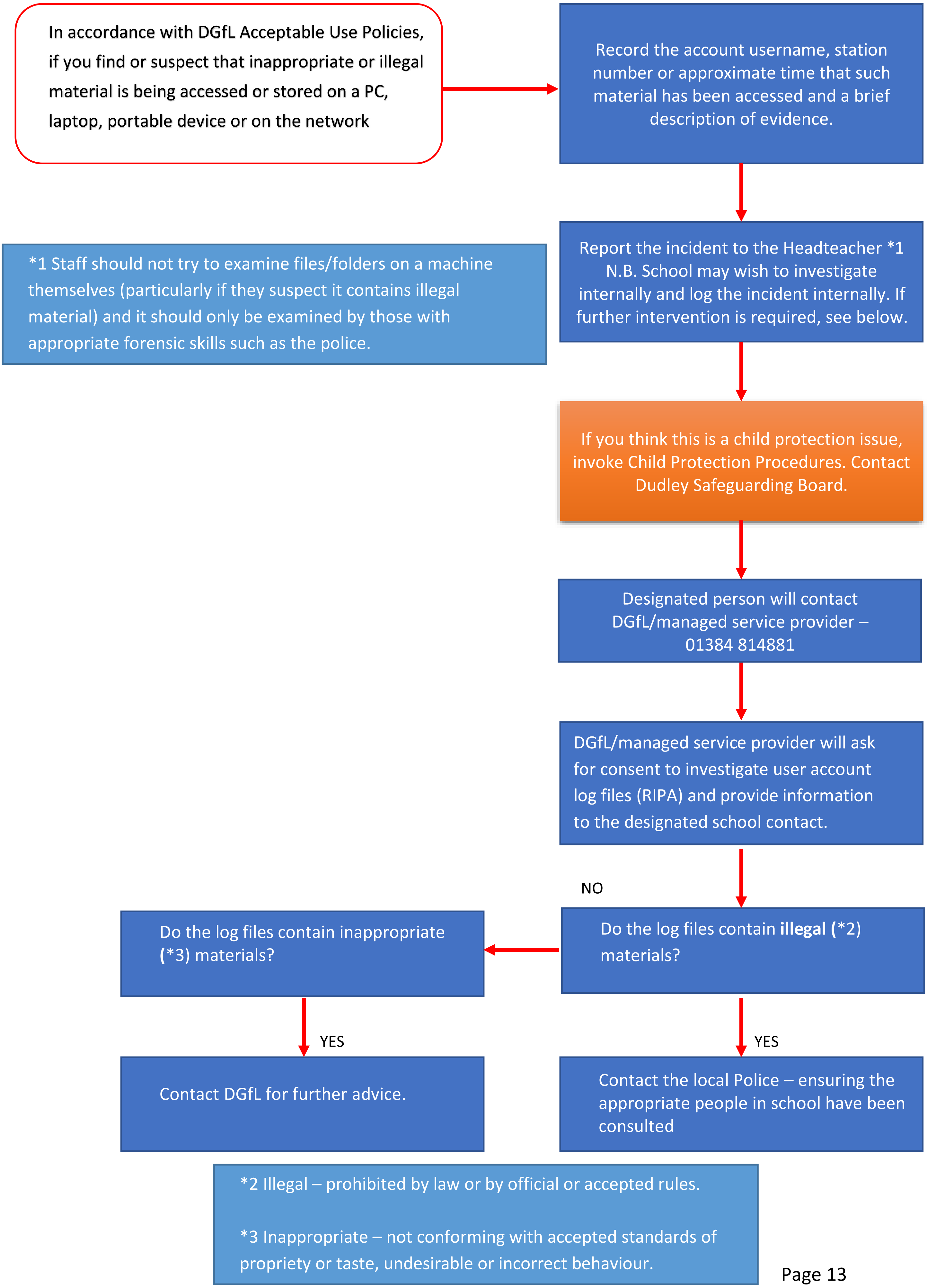
YES

Contact DGfL for further advice.

*2 Illegal – prohibited by law or by official or accepted rules.

*3 Inappropriate – not conforming with accepted standards of propriety or taste, undesirable or incorrect behaviour.

Guidance procedure for E-Safety incidents - Pupil user incidents



In accordance with DGfL Acceptable Use Policies, if you find or suspect that inappropriate or illegal material is being accessed or stored on a PC, laptop, portable device or on the network

Record the account username, station number or approximate time that such material has been accessed and a brief description of evidence.

Report the incident to the Headteacher *1 N.B. School may wish to investigate internally and log the incident internally. If further intervention is required, see below.

*1 Staff should not try to examine files/folders on a machine themselves (particularly if they suspect it contains illegal material) and it should only be examined by those with appropriate forensic skills such as the police.

If you think this is a child protection issue, invoke Child Protection Procedures. Contact Dudley Safeguarding Board.

Designated person will contact DGfL/managed service provider – 01384 814881

DGfL/managed service provider will ask for consent to investigate user account log files (RIPA) and provide information to the designated school contact.

Do the log files contain **illegal** (*2) materials?

NO

Do the log files contain inappropriate (*3) materials?

YES

Contact DGfL for further advice.

YES

Contact the local Police – ensuring the appropriate people in school have been consulted

*2 Illegal – prohibited by law or by official or accepted rules.

*3 Inappropriate – not conforming with accepted standards of propriety or taste, undesirable or incorrect behaviour.

Safety tools available on the DGfL network

E-Safety tool	Type	Availability	Where	Details
RM Safety Net	Web filtering	Provided as part of DGfL	All network connected devices within DGfL	Gives schools the ability to audit, filter and un- filter websites. Provides user-based filtering and access to usage reports for all users.
RM Tutor	Teacher support	Provided as part of DGfL	CC4 desktops	Allows teachers to view and demonstrate screens, control hardware and distribute work
CC4 AUP	Awareness raising	Part of CC4- needs to be enabled	All CC4 stations at log in	When enabled through the management console, users are given an acceptable use policy at log in. If this is rejected, the user is automatically logged off.
eSafe	Forensic Monitoring software	Available to all schools who sign an agreement and attend training	All school owned devices that run a Windows or Chromium operating system.	Takes a snapshot of a screen when an event is triggered. A range of events can be monitored. Proactive incident reporting via an online report or telephone call to the school DSL
Email	Filtering and list control	Provided as part of DGfL	Microsoft O365	Allows schools to restrict where email is sent from/to and filters emails for banned words
Active Directory Fine Grained Password Policy	Safe practice	Provided as part of DGfL3	All CC4 stations	A password management tool that enforces password rules of complexity and length for different users

EYFS Internet Safety Rules

1. I will listen carefully to my teacher about how to use the computer safely.

2. I will only use the computer when my teacher tells me it is okay.

3. I will always show the teacher anything I see that upsets me or I’m unsure about when using the computer

This is how we stay safe when we use computers:

- I will ask an adult if I want to use a computer.
- I will only use activities if an adult says it is ok.
- I will take care of the computer and other equipment.
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
- I will turn off the monitor and tell an adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

I understand these computer rules and will do my best to keep them

My Name	
Signed - child	
Signed - Parent/carer	I have discussed this agreement with my child and believe they have understood the rules.
Date	

Jesson's CE Primary School (VA)

Rules for Responsible Internet Use

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- I will only access the system with my own login and password, which I will keep secret
- I will not access other people's files
- I will only use the computers for schoolwork and homework
- I will use flash drives (memory sticks) appropriately and follow school guidelines on their use
- I will use the Internet safely and sensibly
- When using the internet including a 'chat room' facility, I will not give my home address or telephone/mobile number, respond to requests using SMS or even arrange to meet someone, unless my parent, carer or teacher has given permission
- I will only e-mail people I know, or my teacher has approved
- Files attached to an email should not include any inappropriate materials (something I wouldn't want my teacher to see or read)
- The messages I send will be polite and responsible
- I will always check with a responsible adult before I share or publish images of myself, my friends or other people onto the internet.
- I will report any unpleasant material or messages sent to me. I understand my report would be confidential and would help protect other pupils and myself
- I will not make audio or video recordings of another pupil or teacher without their permission.
- I understand that the school may check my computer files and may monitor the Internet sites I visit
- I will not download any programmes or games on to the school computers, netbooks or laptops unless I have permission to do so.
- I understand that I must not bring my mobile phone into school
- If I do need to bring a personal mobile devices/phone to school then I must not use them for personal purposes within school time. At the beginning of the day the device should be labelled and stored in the school office until it is collected by an adult/pupil at the end of the day. At all times the device must be switched off or onto silent. I understand that I need written permission from a parent to do this

I am aware of the CEOP report button and know when to use it.
I know anything I do on the computer may be seen by someone else.

Parent's/Carer's Signature ………………………………………………

Pupil's Signature ………………………………………………… ***Date*** …………………………………………………

Jesson's Primary School

Acceptable Usage Policy and Security Guidelines

Introduction

This document provides the following guidance to staff working for Jesson's CE Primary School (VA):

1. **Acceptable Usage** – how staff may and may not use school systems and data.
2. **Security** – staff responsibilities for information security.

Scope

These guidelines and policy statements apply to:

- All staff employed by or working in Jesson's CE Primary School (VA).

Purpose and Principles

This policy and accompanying guidelines are designed to enable staff to support the Jesson's CE Primary School (VA) Information Security Policy:

> Jesson's CE Primary School (VA) *is committed to maintaining data integrity, safeguarding confidentiality and controlling the availability of information, in order to achieve education goals effectively and efficiency. We will manage information security so that all applicable legal and regulatory requirements are met, and we will seek to continually improve our information security management systems.*

The information in this document is designed to protect the school, its staff, pupils and parents/carers and other interested parties from the accidental and deliberate misuse of school systems and data. Such misuse might not only lead to interruptions to our school, but could also result in considerable reputational damage and potential legal penalties.

An Acceptable Usage Policy cannot be an exhaustive and complete list of every kind of acceptable and non-acceptable activity within the school environment. Staff are expected to exercise common sense and good judgement in the light of these guidelines, but to seek clarification on any matter about which they do, or could, have doubts.

Use of IT systems and devices

1. Jesson's CE Primary School (VA) provides IT systems and devices for use under the education umbrella. If you are provided with a device for work use, it should be used in accordance with this policy.

2. Limited personal use of systems and devices is allowed during breaks. This includes access to commercial websites but excludes social networking sites. Staff should use their judgement as to the reasonableness of personal use and should consult their line manager if they have any uncertainty. At all times staff are bound by the terms and conditions in their contract.

3. If you have been provided a laptop that you take off the school site it must be encrypted and it is your responsibility to ensure this is done. You can get help to do this by speaking to our ICT technician or calling RM Support on ext 3920.

4. All school located desktops, laptops and tablets should be secured with strong, unique passwords. Passwords should never be shared. Appendix 2 provides guidance on how to create secure passwords.

5. Desktops and laptops should be secured by the use of a password-protected screensaver. When you are away from your desk, the screen of the device should be locked, e.g. Windows Key + L for Windows users.

6. All school owned desktops, laptops and tablets must have anti-virus software installed. This should be the RM recommended software.

7. Rules regarding other software installation will vary across school and so you should consult your manager or LSO (Local Security Officer) about this. However, certain types of software should never be installed on a device handling company data, e.g. torrent software.

8. The software on your device must be properly licensed.

9. Software can be vulnerable to external attacks if it is not kept up-to-date. It is your responsibility to ensure that the latest security patches are installed. If you are in any doubt, contact RM.

10. Personal accounts on cloud-based storage systems, e.g. DropBox, Google Drive, iCloud etc. must not be used to store school or pupil data.

11. Your email address should only be used for work purposes and should be the only email address you use for the creation of logins to work-related systems, unless there is a defined and approved reason not to do so.

12. Staff may share individual files with colleagues using One Drive for Business. Team files should be stored and shared using SharePoint, or the school server (T: drive) with access controlled appropriately.

13. Staff must use their One Drive for Business account, rather than portable storage devices such as external hard drives and USB keys, to back up their personal work files. School or pupil data should never be backed up to personal devices. Where external hard drives or USB keys have been approved for specific business tasks, they must be encrypted when storing or transferring sensitive data.

14. Where staff take school owned devices off-site, they should take appropriate precautions to ensure that the device and its data remain suitably protected, e.g. placing the device so it is out-of-sight when it is not being used at home.

15. Devices that store data (laptop & desktop hard disks, tablets, phones, etc.) must be disposed of securely. RM has a process for secure disposal of such assets, then the asset should be returned to RM.

Use of mobile phones

1. A mobile phone should be treated like any other IT device. If you use a phone for the purpose of work, you must take appropriate security measures in order to protect it.

2. If you are accessing school data via a mobile phone or tablet, you must do the following:

- Set a pin or passphrase, or biometric log such as finger print
- Enable auto lock, so that the screen times out after 1 minute

4. Only install apps from trusted and verified stores/sources.

5. Depending on your type of phone, consider adding additional protection, e.g. an anti-virus/malware app.

Use of personal IT devices

3. A personal IT device should not be used in school unless authorised.

4. If you use a personal device to access school data from home, emails, SharePoint, one drive etc it should be treated like a school IT device. You must take appropriate security measures in order to protect it and the data you access.

5. If you are accessing school data via a personal IT device you must do the following:

    - Set a pin or passphrase, or biometric log such as finger print
    - Enable auto lock, so that the screen times out after 1 minute

6. Ensure you have antivirus installed and up to date as well as any software updates/patches

7. Do not save any data locally to the device. Use One Drive. See the above point about the use of USB sticks.

8. Avoid free hot spots such as coffee shops as you cannot guarantee their security and your traffic can be intercepted.

Unacceptable Use

Unacceptable use includes, but is not limited to, the following:

- Using school systems and devices to access inappropriate sites, forums and tools, e.g. pornographic and gambling sites.

- Unauthorised copying of copyrighted materials.

- Carrying out activities that would constitute harassment, bullying, defamation, discrimination, obscenity, fraud, hacking and other breaches of local or international laws.

- Using school systems to carry out non-school business activities.

- Using personal email addresses for school purposes.

- Using your school email address to authenticate personal online accounts.

- Sharing personal data about school staff, pupils or parents/carers with 3rd parties. The exception for this is for safeguarding purposes. Any emails of that nature must be encrypted by typing ***encrypted:*** at the start of the email subject header.

- Attempting to gain unauthorised access to data.

- Allowing a 3rd party to gain unauthorised access to school data or systems, either whilst on-site or remotely.

- Breaches of the Social Network Policy

Data Classification and Handling

1. Jesson's CE Primary School (VA) has legal and contractual obligations to protect personal, commercial and other types of data.

2. Where security classifications should be applied, data and documents should be classified using this scheme:

   - **Public.** This means the information is not sensitive or confidential.
   - **Confidential.** This means that the information is sensitive or confidential in some way.
   - **Strictly Confidential.** This means that the information is highly sensitive or confidential.

3. How data is stored, transferred and disposed of, should be based on its classification:

   - Printed documents that are Confidential or Strictly Confidential should be disposed of by shredding or by being placed in confidential waste bags.
   - Documents that are Strictly Confidential should be shared internally via One Drive or SharePoint, but where email must be used, e.g. when sending documents to third parties, the attachment should be password-protected.
   - Printed documents that are Strictly Confidential should be sent by secure courier services rather than standard mail.
   - Data that it is Strictly Confidential should be transferred using secure transfer methods, e.g. SFTP.

Data Security

1. Access to other data, and especially sensitive data, is controlled. You should be given the level of access required for your work and job role. If you think you need access to data or a system to which you do not have access, consult with your manager.

2. Documents and portable media containing sensitive information must be locked away at the end of the working day. Checks may be made to ensure that this is done.

3. Any access to systems must be revoked as soon as a member of staff leaves the business.

4. Personal data must be handled in accordance with the data protection legislation. Training will be provided on this legislation where this is appropriate.

Email security

1. Jesson's CE Primary School (VA) uses a range of technical controls to protect you and school devices from malicious email. However, technical controls cannot provide 100% protection: we rely on you to be alert to potential threats and follow this guidance.

2. **Malware.** Emails may contain links or attachments that can install malware on your device.

   To avoid accidentally activating malware in an email:

   - Ensure that your anti-virus software is up-to-date.
   - Don't open attachments or click on links unless the email is from a trusted source.

   You should also ensure that all your personal work files are backed up, i.e. on One Drive.

3. **Phishing emails.** Emails may be sent to you from people trying to trick you into giving them confidential information.

To avoid becoming a victim of a phishing email, be suspicious of:

- Unexpected emails from unknown sources.
- Emails from people asking you for confidential information or access to your computer.
- Emails that contain spelling mistakes, poor grammar or typos.

If you are suspicious of email, look at the sender's email address.

- Has the email address of the company been slightly changed? e.g. new.scotland.yard@met.police.uk has been changed to new.scotland.yard@met.p0lice.uk
- Is the email address from an unlikely domain? e.g. new.scotland.yard@gmail.com not new.scotland.yard@met.police.uk

4. Don't forget that what look like internal emails might be examples of email "spoofing", i.e. someone impersonating a work colleague. If an internal email causes suspicion, then contact them first (call, in person etc) before you open the attachment, click on the link or act on the request.

5. If you do receive a malicious email, mark as Spam, delete the file, and then "double delete" it by emptying your "Deleted Items" folder.

Physical Security

1. You should always report a breach of physical security or a risk of such a breach. Failure to do so can result in significant fines from the information commission.

Reporting

1. All school staff have a responsibility to report known or possible security breaches.

2. Examples of such breaches include, but are not limited to:

   - A breach in physical security at your place of work.
   - The loss of media or devices containing pupil or parent/carer data.
   - A former employee retaining access to school systems.
   - Theft or loss of a school device.

3. Reporting is done by the data protection officer currently provided by Your IG (Dudley council).

Monitoring and Enforcement

1. Jesson's CE Primary School (VA) reserves the right to monitor and audit how staff use school systems and their adherence to this policy.

2. Jesson's CE Primary School (VA) reserves the right to restrict staff access to commercial and non-commercial websites, social networking sites, etc.

3. Disciplinary action may be taken against staff who breach this policy.

4. Should you be aware of another employee who has, or may have, used school systems in a way which breaches any aspect of this policy, you should refer to the Whistleblowing policy.

Further Information

All staff should seek further information if they have any uncertainty about the guidance given above or about any aspect of acceptable usage and information security.

Further information is available from a number of sources:

1. Your manager.
2. Your Local DPO at Dudley Council.
3. HR (Dudley Council).

Password Management

1. All passwords should use the following guidelines (which will be enforced by system rules where possible) to ensure passwords are 'strong' to avoid other people from guessing them.
    - Passwords should not be identical to username, nor shall they have the user or part of their name or full name included within the password.
    - Passwords should not contain personal data (e.g. dates of birth or other significance, names, memorable numbers such as phone numbers).
    - Common passwords should not be used (e.g. 'password', 'qwerty', 'Change me' and so on)
    - Passwords should be at least 10 characters in length.
    - Employees should not" increment" old passwords (e.g. M0nd@y$1, M0nd@y$2, M0nd@y$3 and so on).
    - Passwords should not contain any other easily obtained personal information.
    - Best practice is to link 3 unrelated words such as BlueChairTr33!

2. Employees should at all times keep their personal password confidential, and not share it with anyone (including school employees).

3. A shared login and password is not allowed.

4. Passwords should not be written down or left visible to aid remembrance.

5. Users must not use the same password for School accounts and other personal accounts.

6. The use of free or commercial password safes is permitted.

7. Additional guidance on how to create strong passwords can be found on the Intranet (http://www.dudley.rmplc.co.uk in the information security section)

Appendix 1 - Acceptable Use Policy log sheet

Owner	Business Manager
Approver	Head Teacher
Current Version	V1
Next Review Date	24/03/21

Version History			
Ref	**Changed By**	**Date**	**Comments**

Checks		
Checked By	**Date**	**Comments**

I have/will read and understood the Acceptable Use Policy

Please complete this below		
Staff Name	**Date**	**Signature**

Appendix 2 – Laptop/Chromebook loan/use agreement

It may be necessary for children who are isolating to borrow a laptop or Chromebook from school, to enable them to continue their education remotely. This loan agreement form sets out the acceptable use of the school owned device.

Jesson's CE Primary School (VA)

Helping children be the best they can be.

Laptop loan agreement

1. This agreement is between:

1) Jesson's CE Primary School (VA) ("the school")

School Street

Dudley

DY1 2AQ

2) Parent's name ("the parent" and "I")

Parent's address

and governs the use and care of devices assigned to the parent's child/children (the "pupil(s)"). This agreement covers the period from the date the device is issued through to the return date of the device to the school.

All issued equipment shall remain the sole property of the school and is governed by the school's policies.

1. The school is lending the pupil/pupils a laptop ("the equipment") for the purpose of doing schoolwork from home during COVID-19.

2. This agreement sets the conditions for taking a Jesson's CE Primary School (VA) laptop ("the equipment") home.

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I and the pupil will adhere to the terms of loan.

2. Damage/loss

By signing this agreement, I agree to take full responsibility for the loan equipment issued to the pupil and I have read or heard this agreement read aloud and understand the conditions of the agreement.

I understand that I and the pupil are responsible for the equipment at all times whether on the school's property or not.

If the equipment is damaged, lost or stolen, I will immediately inform Mrs Lea, and I acknowledge that I am responsible for the reasonable costs requested by the school to repair or replace the equipment. If the equipment is stolen, I will also immediately inform the police.

I agree to keep the equipment in good condition and to return it to the school in the same condition when requested.

I will not leave the equipment unsupervised in unsecured areas.

I will make sure my child takes the following measures to protect the device:

- Keep the device in a secure place when not in use
- Don't leave the device in a car or on show at home
- Don't eat or drink around the device
- Don't lend the device to siblings or friends
- Don't leave the equipment unsupervised in unsecured areas
- Keep and use the equipment in a supervised area of your home

3. Unacceptable use

I am aware that the school monitors the pupil's activity on this device.

I agree that my child will not carry out any activity that constitutes 'unacceptable use'.

This includes, but is not limited to the following:

Include details of your acceptable use policy for devices, e.g.:

- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Causing intentional damage to ICT facilities or materials
- Using inappropriate or offensive language

I accept that the school will sanction the pupil, in line with our behaviour policy, if the pupil engages in any of the above **at any time** and the equipment may need to be returned to school.

4. Personal use

I agree that the pupil will only use this device for educational purposes and not for personal use and will not loan the equipment to any other person.

5. Data protection

I agree to take the following measures to keep the data on the device protected.

- Keep the equipment password-protected - strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Make sure my child locks the equipment if it's left inactive for a period of time
- Do not share the equipment among family or friends
- Update antivirus and anti-spyware software as required
- Install the latest updates to operating systems, as prompted

If I need help doing any of the above, I will contact Mr Holmes on the email rholmes@jessons.dudley.sch.uk.

6. Return date

I will return the device in its original condition to Jesson's CE Primary School (VA) office within 7 days of being requested to do so.

I will ensure the return of the equipment to the school if the pupil no longer attends the school.

7. Consent

By signing this form, I confirm that I have read and agree to the terms and conditions set out above.

PUPILS' NAMES	
PARENT'S NAME	
PARENT'S SIGNATURE	

For school use if a signed physical copy is not possible:

By signing this form, I confirm that I have read and agree to the terms and conditions set out above.

COMPUTER/LAPTOP MODEL	
COMPUTER/LAPTOP SERIAL NUMBER	