PACKWOOD HAUGH SCHOOL
(Including EYFS)

E-Safety Policy

Authorised by the Governing Body: Yes Date: 9/10/2023
Produced by: Sue Rigby 01/09/2023
Date Disseminated to the Staff via the intranet: 01/09/2023
Date of Review: 09/10/2024
Signed: James Pitt, Chair of Governors

CONTENTS

APPENDICES

E-Safety Policy

1. Scope

This policy applies to all members of the School community, including staff, pupils, parents and visitors, who have access to and are users of the School IT systems.

For the purpose of this policy:
'Staff' includes teaching and non-teaching staff, governors, and regular volunteers (but access to systems is not intended in any way to imply an employment relationship).
'Parents' include, where applicable, pupils' carers and those with parental responsibility.
'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Both this policy and the Acceptable Use Policies cover fixed and mobile internet devices provided by the School (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto School premises (personal laptops, tablets, smart phones, etc.).

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site, and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place outside of the school but is linked to membership of the school.

The school will, where it becomes known, inform parents/carers of any such incidents of inappropriate online behaviour that takes place out of school.

The 2011 Education Act increased these powers with regard to the searching for electronic devices and the examination of any files or data (even where deleted), on such devices. In the case of both acts, action will be taken in line with the school's published Disciplinary Procedure and/or Behaviour Policy.

The school will keep a record of all staff and students who are granted Internet access. The record will be kept up-to-date and reflect changes or amendments such as a member of staff who has left the school or a student whose access has been withdrawn.

2. Introduction

It is the duty of Packwood Haugh School to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

E-safety is often defined as the safe and responsible use of technology. This includes the use of the internet and also other means of communication using electronic media (e.g. text messages, email, gaming devices etc.).

E-safety is not just about technology, it is also about people and their actions.

Technology provides unprecedented access to new educational opportunities; online collaboration, learning and communication. At the same time, it can provide the potential for staff and students to access material they shouldn't, or be treated by others inappropriately.

E-safety is part of the wider duty of care of all those who work in schools: equipping children and young people to stay safe online, both in school and outside, is integral to a school's Computer Studies curriculum. It may also be embedded in Personal Social and Health Education (PSHE) and Relationship and Sex Education (RSE) and include how pupils should report incidents (e.g. The Child Exploitation and Online Protection (CEOP) button, via a trusted adult, Childline etc.)

General advice and resources for schools on internet safety are available at:
https://www.saferinternet.org.uk/

The use of information and communication technology (ICT) is a vital part of the everyday functioning of and life in school. We also recognise the important role ICT plays in the life of our children and their families.

Whilst there are many benefits and strengths in using ICT there are also a number of risks to children's welfare and safety in school when using internet enabled technology which are summarised in the following categories (Examples of what could be included in the categories if further detailed in KCSIE 2023 Part 2 pages 35-36).

- **Content:** being exposed to illegal, inappropriate, or harmful content.
- **Contact:** being subjected to harmful online interaction with other users.
- **Conduct:** online behaviour that increases the likelihood of, or causes, harm to children or others.
- **Commerce:** illegal, inappropriate, or harmful online commercial activities that can compromise the health and wellbeing or security of children or others.

In association with the appropriate Acceptable Use Policy Agreement (AUP), this policy forms part of the school's commitment to educate and protect all users when accessing digital technologies, both within and outside school. It should be read in conjunction with other relevant policies, such as the Code of Conduct Policy, Data Protection Policy, Health & Safety Policy, Child Protection/ Safeguarding Policy, Behaviour Policy including the Anti-Bullying Policy.

Since 2015 there have been additional duties under the Counter Terrorism and Security Act 2015, known as the ‘Prevent duty’, which require schools to ensure that children are safe from terrorist and extremist material on the internet, to prevent people from being drawn into terrorism.

This policy will be reviewed annually and/or more frequently in line with new developments in the use of the technologies, new threats to online safety or the level and/or nature of incidents reported.

3. The Prevent Duty

As organisations seek to influence young people through the use of social media and the internet, schools and childcare providers need to be aware of the increased risk of online radicalisation and the risks posed by the online activity of extremist and terrorist groups.

The Prevent duty is the duty under the Counter-Terrorism and Security Act 2015 on specified authorities (schools and childcare providers), in the exercise of their functions, to have due regard for the need to prevent people from being drawn into terrorism. The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools.

The general risks affecting children and young people may vary from area to area, and according to their age. Schools and childcare providers are required to identify risks within a given local context and identify children who may be at risk of radicalisation, and know what to do to support them.

The Prevent duty requires school monitoring and filtering systems to be fit for purpose. The school has a filtering system in place and its effectiveness is continuously monitored by the Head of IT and the IT technician.

The Prevent duty means that all staff have a duty to be vigilant, and where necessary, will report concerns about internet use that includes, for example, the following:

- Internet searches for terms related to extremism
- Visits to extremist websites
- Use of social media to read or post extremist material
- Grooming of individuals

All staff should be aware of the following:

1. DfE Prevent duty
2. DfE briefing note on the use of social media to encourage travel to Syria and Iraq
3. The Channel Panel
4. Terrorism Act 2000 and the disclosure of information duty where it is believed or suspected that another person has committed an offence.

Practical advice and information for teachers, parents and school leaders on protecting children from extremism and radicalisation is available at:

https://www.educateagainsthate.com/

The Department for Education has dedicated a telephone helpline (020 7340 7264) to enable staff and governors to raise concerns relating to extremism directly. Concerns can also be raised by email to:

counter.extremism@education.gsi.gov.uk

Please note that the helpline is not intended for use in emergency situations, such as a child being at immediate risk of harm or a security incident, in which case the normal emergency procedures should be followed.

4. Governing Legislation

It is important to note that in general terms an action that is illegal if committed offline, is also illegal if committed online.

Computer Misuse Act 1990
Data Protection Act 2018
Freedom of Information Act 2000
Communications Act 2003
Malicious Communications Act 1988
Regulation of Investigatory Powers 2000
Copyright, Designs and Patents Act 1988
Telecommunications Act 1984
Criminal Justice & Public Order Act 1994
Racial and Religious Hatred Act 2006
Protection from Harassment Act 1997
Protection of Children Act 1978
Sexual Offences Act 2003
Public Order Act 1986
Obscene Publications Act 1959 and 1964
Human Rights Act 1998
The Education and Inspections Act 2006
The Education and Inspections Act 2011
The Protection of Freedoms Act 2012
The Schools Information Regulations 2012
Serious Crime Act 2015
Terrorism Act 2000

Further explanatory detail about governing legislation can be found in Appendix G.

5. Roles & Responsibilities

The Governing Body

The Governing Body of the School is responsible for the approval of this policy and for reviewing its effectiveness. The Governing Body will review this policy at least annually.

E-safety is seen as a 'whole school' issue, with specific responsibilities delegated as follows:

Head	Mr Rob Fox
Member of SMT responsible for e-safety	Mrs Susan Rigby
Head Computer Studies /e-safety co-ordinator	Mr Steve Rigby
IT Manager	Mr Jem Bayliss

A full description of the responsibilities associated with these roles may be found in Appendix F.

6. Definitions: Devices & Technology

Device(s)	Examples include but are not limited to: • Personal computers • Laptops • Tablets • ‘Smart’/Mobile phones • ‘Smart’ watches • Cameras • USB sticks/flash drives
Technology(ies)	Examples include but are not limited to: • Internet search engines • Websites • Social media platforms, e.g. Facebook, Twitter, Instagram, Snapchat, WhatsApp, YouTube • Real time communications e.g. texts, chat rooms, email, instant messaging, Skype, FaceTime, video chat • On-line gaming, e.g. Xbox, PlayStation

7. School Staff, Governors and Volunteers

Acceptable Use Policy Agreements

Before being granted access to school devices and technologies, all members of the school community are required to read and sign an Acceptable Use Policy Agreement (AUP), appropriate to their role and status in school.

The AUP for staff may be used and/or adapted for any user, to include governors and volunteers.

Acceptable Use Policy (AUP) for Staff

The AUP for staff can be found in Appendix A

All staff must read and sign the ‘Acceptable Use Policy Agreement for Staff’ (AUP) before using any school IT resource. These will be stored with the Bursar’s office.

A copy of the staff AUP will be issued to all new members of staff during Induction. The school will also issue the AUP to staff, periodically, in response to the nature and/or volume of reported incidents, changes in legislation and emerging trends in online behaviour.

Access to online services and school devices will not be approved until new staff have signed and returned the AUP. Access may be suspended or restricted for serving staff who do not return an AUP issued on a periodic basis.

Staff are required to accept the general principles of acceptable use of school devices and technologies each time they log in to a school device.

E-safety and the AUP are included in the statutory induction for all new staff and forms part of the contract of employment.

Acceptable Use of Devices and Technologies: Staff

Any device provided by the school, to or for staff or students, is primarily intended to support the teaching and learning of students. Discretion and the highest professional standards of conduct are expected of staff using school devices for personal use.

Where remote access to the school network via a personal device is approved by the Headmaster, staff confirm their acceptance of the terms set out in the Acceptable Use Policy in relation to that device. Staff should seek clarification of any terms and conditions they do not understand.

Staff breaches of the AUP

Where a staff member is found to be in breach of the Staff AUP, the matter will be dealt with in accordance with appropriate school policies such as the Disciplinary procedure, and /or with reference to external agency guidance.

8. Pupils

Acceptable Use Policy (AUP) for Pupils

The AUP for pupils can be found in Appendix B, C & D.

A copy of the pupil AUP is sent to parents with a covering letter, at the start of the academic year, and to new students when they enrol. Pupils will not be given online access or allowed to use school devices before the AUP has been signed and returned to the school office.

It is also available to download on the school website and is displayed in the form rooms.

The pupil AUP will form part of the first lesson of CS for each year group.

The pupil AUPs have been created by the Education Improvement Service. They have been written to be relevant to and appropriate for different age groups, and can be found in Appendices B C and D.

Acceptable Use of Devices and Technologies: Students

Students are required to accept the general principles of acceptable use of school devices and technologies each time they log in to a school device or the school network.

Student breaches of the AUP

Where a student is found to have breached the AUP, this will be dealt with in line with the appropriate school policies, such as the Behaviour policy.

Examples of scenarios which may give rise to an E-safety concern are set out in Appendix I.

Remedial action and sanctions are at the discretion of school management. Outline guidance for teaching and leadership staff is set out in Appendix J.

9. Using non-School Equipment

Under some circumstances, staff, governors and pupils are able to use their own devices in school and connect to the school network.

Regardless of the ownership of the device, the rules and expectations of online behaviour are as set out in the relevant AUP.

10. Security and passwords

Passwords protect the School's network and computer system and are your responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely-used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed, and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.

Staff must always 'lock' a device (e.g. a classroom PC) if they are going to leave it unattended.

NB. The picture 'mute' or picture 'freeze' option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked'.

All users should be aware that the Computer Studies system is filtered and monitored.

11. Data storage

Only encrypted USB pens are to be used in school. For further clarification, please contact Steve Rigby (E-safety Coordinator).

12. Mobile phones, cameras and other devices

The school's policy relating to the use of devices such as mobile phones, is set out in the relevant AUP.

Pupils may not take mobile phones or other electronic devices on school trips.

Pupils should not have mobile phones in school. Those children who are allowed a mobile phone should leave it with the Matrons' Department for safekeeping. Unauthorised phones found in school will be confiscated and taken to the Head.

Confiscated phones can be collected by parents/carers when released by the Head.

If a member of staff suspects that a mobile phone has been misused within the school then it should be confiscated and the matter dealt with in line with normal school procedure and/or the Behaviour policy.

All staff are required to adhere to the AUP and Mobile Phone Policy, which sets out the expected use of mobile phones whilst at School.

Staff should always use a school camera to capture images and should not use their personal devices.

Photographs/Recordings taken by the school are subject to the Data Protection Act.

13. Use of Emails

Pupils and staff should only use e-mail addresses that have been issued by the school and the e-mail system should only be used for school related matters. Staff and pupils should be mindful of the language used in emails and always be respectful of other people. Staff emails are for professional use only and should not be used in a way that is derogatory about others. Pupils and staff are advised to maintain an alternative personal e-mail address for use at home in non-school related matters.

14. Social Media and Networking

The expectations around the use of social media are set out in the relevant AUP.

15. Cyber bullying

All forms of bullying (including cyberbullying) should be handled as a community issue for the whole school. Every school must have measures in place to prevent all forms of bullying. These measures should be part of the school's behaviour policy which must be communicated to all pupils, school staff, governors and parents.

Cyber bullying is defined as '*the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them.*'

Cyberbullying against staff

The DfE state that '*all employers, including employers of school staff in all settings, have statutory and common law duties to look after the physical and mental health of their employees.* This includes *seeking to protect staff from cyberbullying by pupils, parents and other members of staff, and supporting them if it happens*'.

Cyberbullying: Advice for headteachers and school staff is non-statutory advice from the Department for Education for headteachers and all school staff on how to protect themselves from cyberbullying and how to tackle it if it happens.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Please refer to Appendix L for further guidance and support in dealing with instances of cyberbullying against staff and/or pupils.

16. Staff Reporting of E-safety Incidents and Concerns

The school takes the reports of incidents and concerns extremely seriously. Any subsequent action or remedy to be taken following the investigation of an incident or concern, will depend on its nature, situational and circumstantial factors.

All incidents that come to the attention of school staff should be notified to the E-safety Coordinator via the school reporting mechanism set out in Appendix K, or, where applicable, via the Whistleblowing Policy.

Any incident that raises child protection or wider safeguarding questions must also be communicated to the Designated Safeguarding Lead(s) immediately.

Incidents that are of a concern under the Prevent duty should be referred to the E-safety Coordinator and/or Designated Safeguarding Lead, immediately.

Incidents which are not child protection issues but may require SMT intervention (e.g. cyberbullying) should be reported to SMT, immediately.

Examples of potential E-safety concerns may be found at Appendix I.

17. Staff training and updates

All staff have E-safety training included as part of their safeguarding induction to the school and receive regular training in safeguarding pupils. E-safety is included as part of this. Every 2 years the staff receive training from Childnet International. The Governors are invited to attend this training.

E-safety incidents and concerns are a standing item at staff briefings.

18. Communicating the E-safety Policy

Staff and the E-safety policy

- All staff will be given a copy of the E-safety Policy during statutory induction and its importance explained.
- An Acceptable Use Policy Agreement is signed before access to school devices and systems is approved and the agreement forms part of the contract of employment.
- Staff are made aware that emails can be monitored.
- Staff are made aware that internet traffic can be monitored and traced to the individual user, including on personal devices where network access has been granted. Because of this, discretion and professional conduct are essential at all times.

Introducing the E-safety policy to pupils

- The E-safety Policy/Acceptable Use Policy Agreement is/are posted in all classrooms, as appropriate, and its content referred to on a regular basis. The aim is to make the policy familiar and accessible to all pupils at all times.
- Pupils are made aware that network and Internet use is monitored.

Home-School Communication of E-safety information

- The school website provides information on E-safety and how the school can help to support and guide their child
- E-safety advice is included in school letters and as part of the ongoing dialogue between home and school.
- The school holds E-safety events to brief parents and carers about E-safety developments and how to stay safe online.

19. Technical Provision & Safeguards

The school employs an IT technician to oversee the maintenance & running of the school's IT system. All teachers have computers in their classrooms; there are 3 IT suites; the MFL, Acorns & LS departments have ipads. The main server for the system is in the main building where there is also a back-up server. Back-up servers are also placed in two other buildings.

The school uses and internet filtering system at all times (SonicWall) and the security level of the filtering is increased during the pupil's free time limiting the pupils' access to the internet. The filtering includes the blocking of all extremist material in line with the Prevent Duty June 2015. All email is filtered for unsuitable language. Should unsuitable language be used then the email is quarantined and the e-safety co-ordinator & IT technician are notified. If a pupil or member of staff try to access an unsuitable website notification is sent to the e-safety co-ordinator & the IT technician. At regular intervals the e-safety co-ordinator conducts a more thorough check of the use of the internet.

20. Shropshire Safeguarding Contact details:

Local Authority Designated Officer (LADO)	lado@shropshire.gov.uk
Emergency Duty Team	0345 678 9040 01743 249544 (Out of hours only)

21. Monitor & review

This policy will be monitored continuously. It will be reviewed annually, and/or more frequently in line with new developments in the use of the technologies, new threats to online safety or level and/or nature of incidents reported.

Appendix A

Packwood Haugh School
Acceptable User Policy for Staff, Governors & Volunteers

I understand that I have personal and legal responsibilities, including treating others with dignity and respect, acting honestly, using school funds and school equipment appropriately, adhering to health and safety guidelines and safeguarding pupils at all times.

I understand that I must use school devices and systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of systems and other users.

I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to benefit from the use and application of appropriate digital technology.

I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with children and young people.

I will ensure that I comply with the School's e-Safety Policy and other relevant policies, e.g. Retention of Records, Child Protection (Safeguarding) Policy, Behaviour Policy and Data Protection Policy.

Professional and personal safety:

- I understand that the school has in place a filtering system and will monitor my access to digital technology and communications systems whilst using school devices, and/or access to the school network via personal devices, where such access has been granted.
- I understand that the rules set out in this agreement also apply to use of school devices and digital technologies out of school, and to the transfer of personal data (digital or paper based) out of school.

- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use in line with the general principles of this agreement and the expectations of professional behaviour set out in the Staff Code of Conduct.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should keep passwords safe and not share them with anyone. Passwords protect the School's network and computer system and are your responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays); be between 8 and 12 characters long; and nor should they be the same as your widely-used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed, and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.
- I will immediately report any incidence of access to illegal, inappropriate or harmful material, deliberate or accidental, by myself or others, to the appropriate person.
- I will not install or attempt to install programmes of any type on a device, nor will I try to alter computer settings, unless this is permitted by the Head of Computer Studies.
- I will not deliberately disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy and Privacy Notice.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when required by law, or by school policy, to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving devices or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- Any use of personal devices for School purposes, and any removal of personal data or confidential information from School systems – by any means including email, printing, file transfer, cloud or encrypted memory stick – must be registered and approved by the E-safety Co-ordinator.
- I will log out of a device when I have finished using it.

Electronic communications and use of social media:

- I will communicate with others in a professional manner, I will not use aggressive, offensive or inappropriate language and I appreciate that others may have different opinions.
- I will use social networking sites responsibly, taking care to ensure that appropriate privacy settings are in place, and ensure that neither my personal nor professional reputation, nor the school's reputation, is compromised by inappropriate postings, to include past postings.
- I will never send or accept a 'friend request' made through social media from a pupil at school. I understand that such requests should be raised formally as an incident.
- I will not, under any circumstances, make reference to any staff member, pupil, parent or school activity/event via personal social media or other communication technologies.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner. At no time will I use or share a personal email address, phone number or social networking site for such communication purposes.
- I will notify the Headmaster of any current or future, direct or incidental contact with pupils, parents or carers, for example where parents or carers are part of the same social group
- I will not engage in any online activity, at, or outside school, that may compromise my professional responsibilities. This includes making offensive, aggressive or defamatory comments, disclosing confidential or business-sensitive information, or information or images that could compromise the security of the school.
- I will not use the school's name, logo, or any other published material without written prior permission from the Headmaster This applies to any published material, online or in print.
- I will not post any communication or images which links the school to any form of illegal conduct, or which may damage the reputation of the school.

Use of school and personal mobile devices and technologies

- Any property belonging to the School should be treated with respect and care and used only in accordance with any training and policies provided.
- When I use my own mobile device (e.g. laptop / tablet / mobile phone / USB device) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will keep my personal phone numbers private and not use my own mobile phone, or other device, to contact pupils or parents in a professional capacity.

- I will keep my mobile phone secure whilst on school premises. It will be switched to silent whilst I am on duty unless there are good reasons that have been approved with a member of the senior leadership team, and then that is discreet and appropriate, e.g. not in the presence of pupils.
- I will keep mobile devices switched to silent and left in a safe place during lesson times. Mobile phones are not allowed in the classrooms in Packwood Acorns. I understand that the school cannot take responsibility for personal items that are lost or stolen.
- I will report any text or images sent to me by colleagues or pupils which could be viewed as inappropriate. I will not use a personal device to photograph a pupil(s).
- I will not open any hyperlinks in emails or any attachments to emails if I have any concerns about the validity of the email or its source is neither known nor trusted.
- I will, when I take and/or publish images of others, do so with their permission and in accordance with the school's policy on the use of digital/video images. Where these images are approved by the school to be published (e.g. on the school website) it will not be possible to identify by name, or any other personal information, those who are featured.
- I will not share contact details or other information about members of the school community, even if the content is not shared publicly, without going through official channels and obtaining permission.
- I will not attempt to upload, download or access any material which is illegal (for example; images of child sexual abuse, criminally racist material, adult pornography), inappropriate or may cause harm or distress to others. I will not attempt to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not (unless I have permission) make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

Conduct and actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school devices and digital technology in school, but also applies to my use of school systems and equipment off the premises. This Acceptable Use Policy also applies to my use of personal devices on the premises or in situations related to my employment by the school.

I understand that should I fail to comply with this Acceptable Use Policy Agreement, I may be subject to disciplinary action in line with the school's agreed Disciplinary Procedure. In the event of any indication of illegal activity, I understand the matter may be referred to the appropriate agencies.

Retention of Digital Data

Staff, parents and visitors must be aware that all emails sent or received on School systems will be routinely deleted and email accounts will be closed within one year of that person leaving the School.

Important information that is necessary to be kept should be held on the relevant personnel or pupil file, **not** kept in personal folders, archives or inboxes. Hence it is the responsibility of each account user to ensure that important information and/or any personal information that they wish to keep, in line with the School policy on personal use, is retained in the right place or, where applicable provided to the right colleague. That way no important information should ever be lost as a result of the School's email deletion protocol.

If you consider that reasons exist for the protocol not to apply or need assistance in how to retain and appropriately archive data, please contact the Privacy and Compliance Officer (the Bursar).

Breach Reporting

The law requires the School to notify personal data breaches to the authorities and, in some cases, to those affected, if they are likely to cause harm. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This will include almost any loss of, or compromise to, personal data held by the School regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the school's systems, e.g. through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post, fax or email;
- failing to bcc recipients of a mass email; and
- unsecure disposal.

The School must generally report personal data breaches to the ICO (Information Commissioner's Office) without undue delay (i.e. within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the School must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

A suspected breach should be reported immediately to the Privacy and Compliance Officer (the Bursar).

Data breaches will happen to all organisations, but the School must take steps to ensure they are as rare and as limited as possible and that, when they do happen, the worst effects are contained and mitigated. Whilst falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy, failure to report a breach will be a disciplinary offence.

Breaches of this policy

A deliberate breach of this policy will be dealt with as a disciplinary matter using the School's usual procedures. In addition, a deliberate breach may result in the School restricting your access to School IT systems.

If you become aware of a breach of this policy or the e-Safety Policy, or you are concerned that a member of the School community is being harassed or harmed online you should report it to Susan Rigby, DSL & SMT e-safety link.

Reports will be treated in confidence.

I have read and understood the above, and agree to use school devices and access digital technology systems (both in and out of school), as well as my own devices (in school and when carrying out communications related to the school), within this agreement.
I understand that in the event of any query or concern about this Agreement, I should contact the Headmaster.

Staff / Governor/Volunteer Name:	
Signed:	
Date:	

Appendix B –

Acceptable User Policy for learners in KS1

I want to feel safe all the time.

I know that anything I do on the computer can be seen by other people.

I know when to use the CEOP report button

I agree that I will:

- always keep my passwords safe and not share them with anyone
- only open web pages which my teacher has said are OK
- only work with people I know in real life
- tell my teacher if anything makes me feel scared or unhappy on the internet
- make sure all messages I send are polite
- show my teacher if I get a nasty message
- not reply to any nasty message or anything which makes me feel sad or worried
- talk to my teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home, my family or my pets)
- not upload photographs of myself without asking a teacher
- never agree to meet a stranger
- only print off school work to a printer in the IT room/Acorns with the permission of a teacher.

Signed ______________________________ ***Date*** __________________________

Signed ______________________________ ***Date*** __________________________

Appendix C – Acceptable Use Policy (AUP) for KS2 PUPILS

To stay safe when we are using technology, we **must** remember the following:

- I understand that for the safety of myself and others that the school will monitor my use of technology in the school on computers and all other devices.
- I understand that the school will contact my parents/carers if an adult at school is concerned about me or my use of technology.
- I will keep my username and password safe and secure e.g., this means not writing them down or sharing themwith others.
- I will not use anyone else's username and password.
- When I'm using a device, I will only open the app or any other piece of software that my teacher has asked me to open.
- I will not open any links or attachments sent to my email account without checking with a trusted adult or teacher first.
- I will only use school devices when a teacher or trusted adult has given me permission to do so.
- I will make sure I am careful, and I will look after all the devices in my classroom and around the school.
- I will notify a teacher or trusted adult if I notice something on a device isn't working properly or is damaged insome way.
- If I am unsure about anything I am doing on a device, then I will ask a teacher or trusted adult for help.
- If Ihave got something wrong or something surprising has happened on my screen, then I will ask a teacher ortrusted adult for help.
- If I feel upset or worried about anything I see on screen, then I MUST tell a teacher or trusted adult immediately.
- If I see anything that I know is inappropriate on screen, then I MUST tell a teacher or trusted adult immediately.
- When I communicate with others on email or any other messenger service, I will always be careful, kind, respectful, responsible and polite.
- I will not post or share personal information about myself or others online e.g. names, phone numbers, addresses, school name, date of birth, phone numbers etc.
- I will not send or share anything online or in a message that I know could make others feel upset.
- I will be thoughtful about others feelings when I communicate online.
- I will not look up or save anything that I know could make others feel upset.
- I must **never** communicate with strangers online.
- I must **never meet** with strangers that have contacted me online – remember "Stranger Danger!".
- If someone tries to contact me via any kind of message – e.g. email, game chat room, message service etc. – I will tell a trusted adult immediately.
- I understand that if I do not follow these rules, or in any way behave unkindly or inappropriately with technology in school, I may not be allowed to use school devices in the future and my parent/carers will be informed.

Name:

Date: ____

Appendix D – Acceptable Use Policy (AUP) for KS3 PUPILS

What is an AUP?

We ask all children, young people and adults involved in the life of Packwood Haugh School to sign an Acceptable Use* Policy (AUP), which is a document that outlines how we expectthem to behave when they are online, and/or using school networks, connections, internetconnectivity and devices, cloud platforms and social media (both when on school site and outside of school).

Why do we need an AUP?

These rules have been written to help keep everyone safe and happy when they are online orusing technology. Sometimes things go wrong, and people get upset, but these rules help usavoid it where we can.

School systems and users are protected and monitored by security and filtering services toprovide safe access to digital technologies. This means anything you do on a school device or using school networks/platforms/internet (including from home when home learning) may be viewed by one of the staff members who are here to keep you safe.

But it's not about systems and devices – it's about behaviour. So, the same rules apply when youare at school as when you are home learning or just having fun with friends.

All of the points in the list on the next page below can be summarised as follows:

"Treat yourself and others with respect at all times; treat people in the same way when you areonline or on a device as you would face to face."

Where can I find out more?

If you have any questions about this AUP, please speak to Mrs Rigby, Designated Safeguarding Lead / Deputy Head.

What am I agreeing to?

1. I will treat myself and others with respect at all times; when I am online or using any device, I willtreat everyone as if I were talking to them face to face.
2. Whenever I use a device, the internet or any apps, sites and games, I will try to be positive and creative, to learn and share, to develop new skills, to have fun and prepare for the future.
3. I consider my online reputation with everything that I post or share – I know anything I do can beshared and might stay online forever (even on Snapchat or if I delete it).
4. I will tell a trusted adult if I have a problem or am worried about something online, and I willencourage my friends to do so too. Statistics show that telling someone helps!
5. It can be hard to stop using technology sometimes, for young people and adults. When my parents/carers or teachers talk to me about this, I will be open and honest if I am struggling. I willremember the principles of the Digital 5 A Day (Connect, Be Active, Get Creative, Give to Others,Be Mindful).
6. It is not my fault if I stumble across (or somebody sends me) something violent, sexual or otherwise worrying. But I will not share or forward it, and I will ask a trusted adult for advice/help.
7. If I see anything that shows people hurting themselves or encouraging others to do so, I will reportit on the app, site or game and tell a trusted adult straight away.
8. I will ensure that my online activity or use of mobile technology, in school or outside, will not causemy school, the staff, students or others distress or bring the school into disrepute.
9. I will only use the school's internet, systems, devices and logins for school-related activities.
10. Whenever I use the internet or devices in school **OR use school devices at home OR log in on homedevices at home**, I may be monitored or filtered; the same behaviour rules always apply.

11. I will keep logins, IDs and passwords secret and change my password regularly. If I think someoneknows one of my passwords, I will change it; if I think they have used it, I will tell a teacher.
12. I will not try to bypass school security in any way or access any hacking files or tools.
13. I will only edit or delete my own files and not (even try to) view, change or delete other people's files or user areas without their permission.
14. I will use the internet, apps, sites & games responsibly; I will not use any that are inappropriate forschool use or for my age, including sites which encourage hate or discrimination.
15. I understand that any information I see online could be biased and misleading, so I should alwayscheck sources before sharing (see fakenews.lgfl.net for support).
16. I understand that bullying online or through using technology is just as unacceptable as any other type of bullying, and I will not use technology to bully, impersonate, harass, threaten, make fun ofor upset anyone, at school or outside. I will stand up for my friends and not be a bystander.
17. I will not post, look at, up/download or share material that could be offensive, harmful or illegal. IfI come across any, I will report it immediately.
18. I know some sites, games and apps have age restrictions (most social media are 13+) and I shouldrespect this. 18-rated games are not more difficult but are inappropriate for young people.
19. When I am at school, I will only message or mail people if it's relevant to my learning and I will onlyuse my school email address.
20. Messages I send, or information I upload, will always be polite and sensible. I understand that allmessages I send reflect on me and the school.
21. I will be careful when opening files and attachments, checking for viruses etc. If I am unsure I willnot open a file, hyperlink or any other attachment.
22. I will not download copyright-protected material (text, music, video etc.).
23. I will not share my, or others', personal information that can be used to identify me, my family ormy friends on any online space, unless a trusted adult has given permission or reviewed the site.

24. Livestreaming can be fun, but I always check my privacy settings and know who can see whatand when. If I livestream, my parents/carers know about it.
25. I know new online friends might not be who they say they are, so I am always very careful when someone wants to 'friend' me. Unless I have met them face to face, I can't be sure who they are.
26. I will never arrange to meet someone face to face who I have only previously met in an app, site or game without telling and taking a trusted adult with me.
27. **When learning remotely, teachers and staff will not behave any differently** to when we are inschool. If I get asked or told anything that I would find strange in school, I will tell another teacher.
28. I will only use my personal devices (mobiles, smartwatches etc) in school if I have been givenpermission, and I will never take secret photos, videos or recordings of teachers or students,**including when learning remotely.**
29. I will respect my body and other people's – part of that means using positive words about myselfand others; it also means not revealing too much on camera and not sharing or posting photos orvideos that show me or anyone else without all of my/their clothes on.
30. Many apps can identify where I am or where I made a post or took a photo, so I know how to turnoff location settings, so everyone doesn't see where I am, where I live or go to school.
31. What I do on devices should never upset or hurt others & I shouldn't put myself or others at risk.
32. If I see, watch, read, hear or receive anything I am unhappy with or I receive a message thatmakes me feel uncomfortable, e.g., bullying, sexual, extremist/hateful content, I will not respond to it but I will talk to a trusted adult about it.
33. I don't have to keep a secret or do a dare or challenge just because someone (even a friend)tells me to – real friends don't put you under pressure to do things you don't want to.
34. It is illegal to view any form of pornography if you are under 18 years old; I will not attempt to doso and will report anyone who tries to trick me into doing so.
35. I can always say no online, end a chat or block someone; if I do, it's best to talk to someone aboutthis, too.
36. I know who my trusted adults are at school, home and elsewhere, but if I know I can also get intouch with Childline, The Mix, or The Samaritans.

I have read and understand these rules and agree to them.

Signed:________________________ **Date:** ___________________

Appendix E– *Sample Home-school E-safety; Computer Studies, Mobile Phones, Personal Photographs and Social Media*

Pupil Name	
Pupil’s form teacher/form name	
Parent/Carer/Guardian’s name	

Use of School Computer Studies Equipment and Internet Access

As the parent or legal guardian of the above-named pupil, I give permission for my child to access the Internet, the Virtual Learning Environment, school email and other Computer Studies facilities, whilst at school. I understand that my child has signed an Acceptable Use Policy (AUP) confirming their understanding and acceptance of the proper use of school and personal Computer Studies equipment. I also understand that my child may be informed, should the rules change or be updated, during the year.

I accept that ultimately, the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep students safe and to prevent them from accessing inappropriate materials. These steps include the school using a filtered internet service, providing secure access to email, employing appropriate teaching practice and teaching e-safety skills to students, across the curriculum.

I understand that the school can monitor my child’s computer files and the Internet sites they visit. I also understand that the school may contact me if there are concerns about my child’s online behaviour or safety. I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns about my child’s e-safety.

Mobile Phones and other Personal Devices

I understand that unless my child is given permission by a teacher, mobile phones and other electronic devices are not allowed in school. This includes during off-site activities. If my child breaks this rule, I understand that the phone or device will be confiscated, and I will be asked to collect it in person from the Headmaster

I understand that ‘Smart’ watches must not be brought to school under any circumstances.

Personal Photographs and Social Media

I am aware that the school permits parents/carers to take photographs and videos of their own children at school events but requests that where the photos/videos contain images of other children, these are not shared on any social networking site such as Facebook or Instagram. I will support the school's approach to e-Safety and will not post, upload or add any text, image or video that could upset, offend or threaten the safety of any member of the school community

Signature of Parent/Carer/Guardian:

Date:

Appendix F: E-safety Roles & Responsibilities: List of duties

The Head and Member of SMT with responsibility for e-safety	• Has overall responsibility for E-safety provision. • Ensures that the school uses an appropriate filtered Internet Service • Ensures that staff receive appropriate training to enable them to carry out their E-safety roles • Can direct the whole school community including staff, students and governors to information, policies and practice about E-safety. • Is aware of the procedures to be followed in the event of a serious E-safety incident. • Receives regular monitoring reports from the E-safety Coordinator • Ensures that there is a system in place to monitor and support staff who carry out internal E-safety procedures and reviews (e.g. Network Manager). • Oversees the administration of the staff Acceptable Use Policy Agreements and takes appropriate action where staff are found to be in breach. • Ensures that the school is compliant with all statutory requirements in relation to the handling and storage of information. • Ensures that any recording, processing, or transfer of personal data is carried out in accordance with the *Data Protection Act* 2018.
E-safety Coordinator /Head of IT	• Takes day to day responsibility for E-safety issues and assumes a leading role in establishing and reviewing the school E-safety policies and supporting documents. • Promotes an awareness of and commitment to E-safety throughout the school community. • Ensures that E-safety is embedded across the curriculum. • Is the main point of contact for students, staff, volunteers and parents who have E-safety concerns. • Ensures that staff and students are regularly updated on E-safety issues and legislation, and are aware of the potential for serious child protection issues that arise from (for example): - sharing of personal data - access to illegal/inappropriate materials - inappropriate on-line contact with adults/strangers - cyber-bullying • Ensures that all staff are aware of the procedures that need to be followed in the event of an E-safety incident. • Ensures that an E-safety incident log is kept up to date. • Liaises with school IT technician where necessary and/or appropriate. • Facilitates training and provides advice and guidance to all staff. • Communicates regularly with SMT to discuss current issues, review incident logs and filtering.

Head of Computer Studies	• Oversees the delivery of the E-safety element of the Computing curriculum. • Communicates regularly with the SMT E-safety coordinator.
Network Manager/Technician	• Oversees the security of the school Computer Studies system. • Ensures that appropriate mechanisms are in place to detect misuse and malicious attack (e.g. firewalls and antivirus software). • Ensures that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • Ensures that the school's policy on web-filtering is applied and updated on a regular basis. • Ensures that access controls/encryption exist to protect personal and sensitive information held on school-owned devices. • Ensures that users may only access the school networks through an authorised and properly enforced password protection policy. • Reports any E-safety incidents or concerns, to the E-safety co-ordinator. • Keeps up to date with the school's E-safety policy and technical information in order to carry out the E-safety role effectively and to inform and update others as relevant. • Keeps up-to-date documentation of the school's E-security and technical procedures. • Keeps an up to date record of those granted access to school systems.
ALL Staff	• Are required to sign the AUP before accessing the School's systems. • Read, understand and help promote the school's E-safety policies and guidance. • Are aware of E-safety issues relating to the use of any digital technology, monitor their use, and implement school policies with regard to devices. • Report any suspected misuse or problem to the E-safety coordinator. • Maintain an awareness of current E-safety issues and guidance, e.g. through training and CPD. • Model safe, responsible and professional behaviours in their own use of technology. • Ensure that any digital communications with students are on a professional level and through school-based systems ONLY. • Ensure that no communication with students, parents or carers is entered into through personal devices or social media. • Ensure that all data about pupils and families is handled and stored in line with the principles outlined in the Staff AUP.
Teaching Staff	• Embed E-safety issues in all aspects of the curriculum and other school activities. • Supervise and guide students carefully when engaged in learning activities involving online technology (including extracurricular and extended school activities, where relevant). • Ensure that pupils are fully aware of how to research safely online and of potential legal issues relating to electronic content such as copyright laws.

Pupils	• Are responsible for using the school digital technology systems in accordance with the Pupil AUP Agreement. • Have a good understanding of research skills, the need to avoid plagiarism and to uphold copyright regulations. • Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. • Understand policies on the use of mobile devices and digital cameras, the taking and use of images and cyber-bullying. • Understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions, in and out of school, if related to their membership of the school.
Parents / Carers	Parents and carers are encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of: • digital and video images taken at school events. • access to parents' sections of the website and on-line pupil records. • their children's personal devices in the school. (where this is allowed)
External groups	Any external individual/organisation must sign an Acceptable Use Policy prior to using any equipment or the Internet within the school.

Appendix G: Legislation - Overview of relevant legislation governing E-safety

Schools should be aware of the legislative framework under which this E-safety Policy template and guidance has been produced. It is important to note that in general terms, an action that is illegal if committed offline is also illegal if committed online.

It is recommended that HR and/or legal advice is sought in the event of an E-safety incident or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998 and 2018

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence, liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority, intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
    - Ascertain whether the communication is business or personal;
    - Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this Act.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as ‘fair dealing’, which means, under certain circumstances, permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear, on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet), it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification, or that of others. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any person having sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view to releasing it, a criminal offence.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems.

The School Information Regulations 2012

Requires schools to publish certain information on its website:
https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015

Introduced the new offence of sexual communication with a child. Also created new offences and orders around gang crime (including Child Sexual Exploitation (CSE)).

Appendix H: *E-Safety Incident Reporting Log*

Date	*Time*	*Incident*	*Action Taken*		*Incident Reported By*	*Signature*
			What?	*By Whom?*		

Appendix I: Examples of potential E-safety concerns (Students)

The following are provided by way of guidance and are in no way limiting or exhaustive. You should seek advice from the E-safety coordinator if you are unsure about what might constitute a concern.

Inappropriate material accessed on school computers

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 computer even when filtering is in place and users abide by the rules.

Pupils are taught that they are not at fault if they see or come across something online that they find worrying or upsetting and are encouraged to alert staff to any inappropriate content. The staff member should report the incident to the E-safety Co-ordinator who will log the problem and liaise with the IT technician to make any necessary adjustment to filter settings.

Abusive messages on school computers

Pupils who receive abusive messages over school systems will be supported, and advised not to delete messages. The E-safety Co-ordinator will be informed and a formal process of investigation initiated.

Parent/Carer/Guardian reports of cyber bullying

Parents, carers and guardians may become aware that their child is concerned or upset by bullying, originating in the school but continuing via electronic means. Parents and carers should know that the school encourages them and/pupils to approach them for help, either via a staff member or directly to the Head. Such incidents will be investigated and dealt with in accordance with the school/academy Behaviour/Bullying policy.

Pupil disclosure of concerns or abuse

All staff receive Safeguarding and E-safety training as part of their induction, and thereafter on a regular basis. Where a student discloses a concern to a member of school staff, this is passed on to the Designated Safeguarding Lead and, where appropriate, the E-safety Coordinator.

Pupil reporting outside school

Pupils are taught that if something worries them, or if they think a situation is getting out of hand, that they should share this with a trusted adult such as their parents, carers, guardians or school staff.

Allegations against staff

Allegations involving staff should ordinarily be reported to the Headteacher or through the Whistleblowing Policy. If the allegation is one of abuse then it should be handled in line with the statutory DfE guidance: ‘Dealing with allegations of abuse against teachers and other staff’. If necessary local authority’s LADO should be informed.

Evidence of incidents must be preserved and retained and where necessary, the LADO informed.

The curriculum will cover how pupils should report incidents (e.g. CEOP button, trusted adult, Childline)

Appendix J: How to Manage Student Breaches of the Acceptable Use Policy

Where a student is found to have breached the AUP, this will be dealt with in line with the appropriate school policies, such as the Behaviour policy.

Remedial action relating to potential sanctions is at the discretion of school management as suggested as below.

The following are provided as exemplification only, and should be amended and/or confirmed by the school, as appropriate:

Level 1 breaches

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other devices/technologies) in lessons, e.g. to send texts to friends
- Use of unauthorised instant messaging/social networking sites

Possible Sanctions:

- refer to class teacher / e-Safety Coordinator
- confiscation of phone or other device

Level 2 breaches

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile phone (or other devices/technologies) after being warned
- Continued use of unauthorised instant messaging/social networking sites
- Use of Filesharing software
- Accidentally corrupting or destroying others' data without notifying a member of staff
- Accidentally accessing offensive material and not notifying a member of staff

Possible Sanctions:

- refer to Class teacher/ E-safety Coordinator
- removal of Internet access rights for a period
- confiscation of phone or device
- contact with parents/carers

Level 3 breaches

- Deliberately corrupting or destroying someone’s data, violating the privacy of others
- Sending an email and/or message that is regarded as harassment or of a bullying nature (cyberbullying)
- Deliberately trying to access offensive or pornographic material

Possible Sanctions

- refer to Class teacher / E-safety Coordinator / Headteacher
- removal of Internet rights for a period
- contact with parents/carers

Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site
2. Inform SSCB/LA as appropriate

Level 4 breaches

- Continued sending of emails and/or messages regarded as harassment or of a bullying nature after being warned (cyberbullying)
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1998 & 2018
- Bringing the school name into disrepute

Possible Sanctions:

- Referred to Head Teacher
- Contact with parents
- possible exclusion
- refer to Community Police Officer / LA e-safety officer

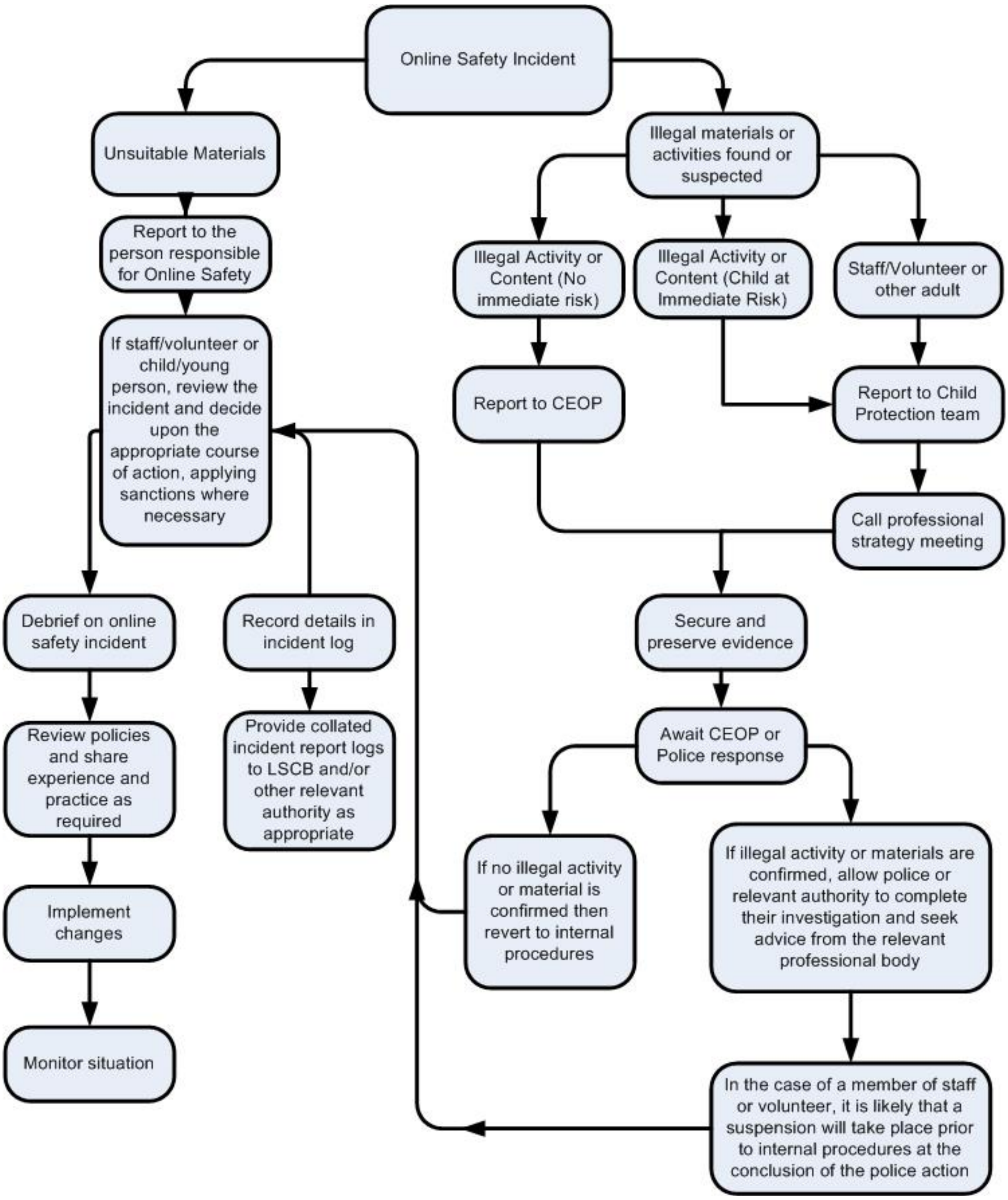
Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender’s e-mail service provider if a system other than the school system is used.

Pupils are also informed that sanctions can be applied to e-safety incidents that take place out of school, if they are related to school or any member of its community.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and collect data evidence and/or the Local Authority Human Resources team.

Appendix K: Recording and Responding to incidents of misuse – flow chart


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

Appendix L: Cyberbullying: further advice and guidance

Behaviour that is classed as cyber bullying includes but is not limited to:

- **Abusive comments**, rumours, gossip and threats made over the internet or using digital communications – this includes internet trolling.

- **Sharing pictures**, videos or personal information without the consent of the owner and with the intent to cause harm and/or humiliation.

- **Hacking** into someone's email, phone or online profiles to extract and share personal information, or to send abusive or inappropriate content whilst posing as that person.

- **Creating specific websites or 'pages' on the Internet** that negatively target an individual or group, typically by posting content that intends to humiliate, ostracise and/or threaten.

- **Blackmail**, or pressurising someone to do something online they do not want to do such as sending a sexually explicit image.

Cyberbullying: Advice for headteachers and school staff

The Department for Education has produced non-statutory advice for headteachers and all school staff on how to protect themselves from cyberbullying and how to tackle it if it happens.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Preventing and tackling bullying: Advice for headteachers, staff and governing bodies

This document has been produced by the Department for Education to help schools take action to prevent and respond to bullying as part of their overall behaviour policy. It outlines, in one place, the Government's approach to bullying, legal obligations and the powers schools have to tackle bullying, and the principles which underpin the most effective anti-bullying strategies in schools. It also lists further resources through which school staff can access specialist information on the specific issues that they face. This includes cyberbullying.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/623895/Preventing_and_tackling_bullying_advice.pdf

(a) Shropshire Council Advisory Service documentation
All Advisory Service e-safety documentation can be found at:
https://www.shropshirelg.net/esafety/staff/Pages/welcome.aspx

(b) The Safe Use of New Technologies
The Safe Use of New Technologies report is summary of findings from OFSTED based on 35 e-safety inspections carried out in a range of settings. http://bit.ly/9qBjQO

(c) 360 degree Safe
The policy guidance is based upon criteria with the 360 degree safe framework. The framework can be found at: http://www.360degreesafe.org.uk