THE OLD POST OFFICE
WELLBEING HUB

Online Safety and ICT Acceptable Use Policy

Introduction

The Old Post Office Wellbeing Hub (the venue) is a for-profit Organisation run for the following purpose:

The Old Post Office Wellbeing Hub is a purpose-built space designed to be used by groups to enhance the wellbeing of children and young people, parents and carers, and professionals working in education.

The Old Post Office C.I.C. (the Organisation) is a not-for profit organisation which provides support for children, young people (and their families) who are struggling to attend mainstream education.

The Organisation is based at:

Springlands Farm, London Road, Mountfield, East Sussex. TN32 5LX.

The Organisation has adopted this 'Online Safety and ICT Acceptable Use Policy' and expects every service provider, working or helping at The Old Post Office Wellbeing Hub to support and comply with it. Consequently, this policy shall apply to all service providers, service users, volunteers and people using or renting the venue.

This policy supports the aims The Old Post Office Wellbeing Hub and The Old Post Office C.I.C. in educating learners to explore horizons in line with the digital world safely and setting up a safety net for service providers and service users.

This policy applies to all service providers, pupils, parents, and visitors and includes use of the venue's internet access. All service providers are responsible for service users' computer / device usage, and that they access the venue's internet inline with this policy. All service providers and service users are expected to adhere to this policy.

Rationale

Information Technology includes a wide range of resources including web-based, mobile, and blended learning. It is important to recognise the constant and fast paced evolution of IT within our society as a whole. Currently the internet technologies children and young people are using inside and/or outside of the classroom include:

● Websites

● Learning Platforms, Virtual Learning Environments, Artificial Intelligence

● E-mail and Instant Messaging

● Chat Rooms

● Social Networking

● Cloud computing, such as Google Drive, iCloud Drive and OneDrive

● Blogs and Wikis

● Podcasting

- Video Broadcasting

- Music Streaming and/or Downloading

- Film or TV streaming

- Gaming

- Mobile devices, such as Chromebooks, Laptops, iPADs, Tablets, etc.

- Mobile/Smart phones with text, video and/or web functionality

- Other mobile devices with web functionality, including Apple Watches.

Whilst exciting and beneficial, both in and out of the context of education, much IT, particularly web-based resources, are not consistently monitored. All users need to be aware of the range of risks associated with the use of these digital technologies. The Old Post Office Wellbeing Hub and The Old Post Office C.I.C. understand the responsibility to educate children about the importance of online safety issues; helping them to raise their awareness and develop the appropriate behaviours and critical thinking skills to enable them to remain both safe and within the law when using the internet and related technologies, in and beyond the context of the classroom. Building these important skills and strategies, will help them to become model digital citizens in a complex world ahead.

This policy and the Computer/Device Usage Agreements for all service providers and pupils (see Appendix 1, 2, 3 and 4) apply to technologies and accounts provided by The Old Post Office Wellbeing Hub and The Old Post Office C.I.C.. PCs, and to technologies owned by service providers and service users, brought onto the premises (such as chromebooks, laptops, mobile devices, tablets, portable media players and any other internet enabled device).

ROLES AND RESPONSIBILITIES

Anita Auer is the Designated Safeguarding Lead and endeavours to keep abreast of current issues and guidance through organisations such as the DfE, CEOP (Child Exploitation and Online Protection), NSPCC and Childnet.

This policy is to protect the interests and safety of all service providers and service users; it is linked to the The Old Post Office policies listed at the end of this policy.

MONITORING

The Old Post Office Wellbeing Hub has appropriate filters and monitoring in place as part of our obligation to comply with Keeping Children Safe in Education and the Prevent Duty.

Anita Auer is constantly reviewing industry trends to improve filtering and monitoring of internet use in accordance with Keeping Children Safe in Education and any other Department for Education and online safety statutory guidance.

Only service providers are given the access codes to the venue's internet access.

The Old Post Office Wellbeing Hub and The Old Post Office C.I.C recognise that service providers and service users can access the internet over mobile phone operators 3G/4G/5G connections. Children are asked to store their mobile phones when learning. Parents are advised to make use of the filtering and monitoring facilities provided by their mobile phone operator on these connections, and ensure that their children are taught how to keep themselves safe online. The Old Post Office Wellbeing Hub shares regular safe-guarding updates on their social media and to parents, to promote online safety and e-safety awareness.

PUPILS

Inclusion: The Old Post Office endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of their online safety guidelines and regulations.

However, service providers are aware that some service users may require additional support, including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of online safety issues.

Careful consideration is given to group interactions when raising awareness of online safety. Internet activities are carefully planned and well managed.

Education: IT and online resources are increasingly used across all areas of the curriculum.

We believe it is essential for online safety guidance to be given to the service users on a regular and meaningful basis, so this is embedded in our curriculum as appropriate.

Service users are made aware of the relevant legislation when using the internet such as data protection, digital footprint, and intellectual property which may limit what they choose to do but also serves to protect them.

Service users are taught about digital citizenship, copyright, and the importance of respecting other people's information, images, and opinions, through collaborative discussion and activities.

Service users are aware of the impact of cyberbullying/online bullying and know how to seek help if they are affected by any form of cyberbullying. They are also made 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 service provider member, or an organisation such as Childline, NSPCC or CEOP.

Service users are taught to critically evaluate digital resources and materials, and to build effective and efficient online searching skills through cross-curricular teacher models and discussions.

The Old Post Office works closely with parents to help them support the online safety of their children.

Email: The use of email within most educational establishments is an essential means of communication for both service providers and pupils. We recognise that service providers and service users need to understand how to appropriately style an email in relation to their age, their audience, and with good network etiquette.

All service users are expected to adhere to the generally accepted rules, particularly in relation to the use of appropriate language, not revealing any personal details about themselves or others in email communication (e.g. name, date of birth, address, telephone number, etc.), not arranging to meet anyone without specific permission, and checking for/ not opening virus attachments/links.

Internet Usage: The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Any use of the internet at The Old Post Office is only made possible by the service provider. The service provider should monitor the service users use of the internet and whenever any inappropriate use is detected it will be followed up.

The following rules should be followed:

● Unplanned image searches are discouraged when working with children.

● All users must observe software copyright at all times. It is illegal to copy or distribute The Old Post Office software or illegal software from other sources.

● All users must observe copyright of materials from electronic resources, including Google image searches.

● Users must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience.

● Online gambling is not allowed.

● Access to websites that could be categorised as "adults only" is not permitted, even if the service user is over the age of 18.

● Service users are aware that internet activity will be monitored and explored further if required.

● The Old Post Office has parental controls and anti-virus on all laptops.

It is not The Old Post Office's responsibility to install or maintain virus protection on any personally-owned devices.

Removable media (personal or for The Old Post Office use) should not be used on The Old Post Office devices.

Service Users are not permitted to download programs on venue-based technologies.

Service users must never interfere with any monitoring software installed on the The Old Post Office's IT equipment.

If there are any issues related to viruses or anti-virus software, Anita Auer should be informed immediately.

Social Media: Social media, if used responsibly both outside and within an educational context, can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism.

To this end, we encourage our service users to carefully reflect about the way that information can be added and removed by all users, including themselves, from these sites. Information, which is captured by third parties, automatically or through 'cookies' consent, can be stored as part of their digital footprint, transferred externally and/or used within advertisement frameworks to build digital profiling.

Service users should not access social media while within The Old Post Office without permission of the service user.

All service users are advised to be cautious about the information given by others on sites, for example users not being who they say they are. They are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image from their digital footprint. It is important to remember that anything and everything may always be captured when connecting online, including the sites visited.

Service users are always reminded to avoid giving out personal details on any websites which may identify them or where they are (full name, address, mobile/home phone numbers, The Old Post Office details, IM/email address, specific hobbies/interests, etc).

Service users are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.

Service users are encouraged to be wary about publishing specific and detailed private thoughts and opinions online, especially where they may intentionally or unintentionally cause others harm.

Service users are advised to carefully read the Terms and Conditions, including any age restrictions on the use of any website before signing up. Pupils are equally encouraged to check with a trusted adult, if unsure about the safety or any website, before registering to join any online community.

Inappropriate Material: Accidental access to inappropriate materials must be immediately reported to a DSL.

Deliberate access to inappropriate materials must be reported to a DSL and will be logged. Depending on the seriousness of the offence, the DSL will contact SPOA and there will may be involvement of police for very serious offences.

Viruses: Service users must never interfere with any anti-virus software installed on The Old Post Office IT equipment.

If service users suspect there may be a virus on any venue IT equipment, they must stop using the equipment immediately and tell the service provider. The service provider will advise what actions are to be taken and are responsible for advising others who need to know.

Mobile Devices: With permission from the service provider, children over the age of 11 are allowed to bring personal mobile devices into the venue but should not be used in sessions without permission and, when used, should be done so responsibly.

Issue or concerns: Issues or concerns relating to online safety should be referred to the DSL. Incident s will be logged and The Old Post Office procedure for investigating online safety/incidents will be followed.

SERVICE PROVIDERS

Monitoring: Deliberate and serious breach of the policy statements in this section will lead to the service provider being barred from the venue.

All of The Old Post Office's IT equipment, devices, phone, internet and email related resources are provided for business purposes. Therefore, the organisation maintains the right to monitor internet and network traffic, together with the email systems. The specific content of any transactions may be monitored, investigated and/or used in order to meet The Old Post Office's obligations regarding monitoring and filtering arrangements; if there is a suspicion of improper use; to confirm or obtain The Old Post Office's business-related information; to confirm or investigate compliance with The Old Post Office's policies, standards and procedures (including safeguarding); to ensure the effective operation of The Old Post Office IT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 2018, or to prevent or detect crime.

The owners of The Old Post Office may, without prior notice, access the email, or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

Service providers should always exercise caution when committing confidential information to email since the confidentiality of such material cannot be guaranteed. The Old Post Office reserves the right to monitor electronic communications in accordance with applicable laws and policies. The right to monitor communications includes messages sent or received by system users (employees, volunteers and temporary employees) within and outside the system as well as deleted messages.

PCs and Other The Old Post Office Equipment: A user of IT is responsible for any activity undertaken on The Old Post Office's IT equipment provided.

Equipment must be kept physically secure in accordance with this policy. When travelling by car, best practice is to place the laptop in the boot of a car before starting a journey.

The installation of any applications or software packages must be authorised and carried out by the the owners of The Old Post Office. Portable or mobile IT equipment must not be left unattended and any personal data and/or confidential information must be kept secure. Portable equipment must be transported in its protective case if supplied.

Data Security: guidelines, responsibility and management of data

The accessing and appropriate use of The Old Post Office data is something that The Old Post Office takes very seriously. Service Providers are required to follow the Online Safety and ICT Acceptable Use Policy and the Privacy Policy. It is the responsibility of individual service providers to ensure the security of any personal, sensitive, confidential and classified information. Any individual service provider who produces any electronic documents that contain personal data are responsible for ensuring secure storage and/or disposal.

Personal data sent or received via email must be downloaded only via agreed channels to a designated storage device. Service providers must ensure that any personal data stored on any device or memory stick is password protected, including personal devices.

PCs, laptops, chromebooks and/or tablets must be locked or switched off when away from desks/workstations.

Electronic files must be securely deleted and service providers should manage their download files either by deleting the files once they have been viewed and are no longer needed or visiting their download folder once a month and deleting files no longer required.

All service providers should log off or lock a device that they are using before leaving it unattended.

Breaches

In the event of any data breach, this must be reported immediately to Anita Auer (DSL).

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 service provider regardless of whether the personal data falls into a third party's hands.

The Old Post Office must generally report a data breach to the Information Commissioner's Office (ICO) without undue delay and within 72 hours if it presents a risk to individuals. In addition, the service provider must notify individuals affected if that risk is high. In any event, the Old Post Office must keep a record of any personal data breaches, regardless of whether there is a need to notify the ICO.

Response to a Breach of Policy

A deliberate breach of this policy will be dealt with as a disciplinary matter using The Old Post Office's usual procedures. In addition, a deliberate breach will probably result in The Old Post Office preventing the service user from working within The Old Post Office.

Incident reporting

Any breach that may be a breach of personal data must be reported immediately, following the procedure above and within the Data Protection Guidance for service providers.

Any attempted or successful security breaches, loss of equipment, unauthorised use or suspected misuse of IT, security breaches, lost/stolen equipment or data, virus notifications, misuse or unauthorised use of IT and any other policy non-compliance must be reported to Anita Auer.

All online safety incidents involving either service users or providers will be recorded by the Designated Safeguarding Lead (Anita Auer).

Inappropriate material

All users are aware of the procedures for reporting accidental access to inappropriate materials. Any access to inappropriate materials must be reported to the DSL (Anita Auer) and logged. Depending on the seriousness of the offence, there will follow: investigation by Anita Auer, immediate suspension from service providers from running sessions within The Old Post Office, possibly leading to termination and involvement of police for very serious offences.

Where the allegation(s) concern Mrs Auer, the service user or provider should speak to the LADO or police.

Viruses

Anti-virus software must be installed on all IT equipment used within The Old Post Office or their service providers, and it must not be interfered with.

If a user suspects there may be a virus on anyl IT equipment, they must stop using the equipment and get advice on what actions to take and be responsible for advising others who need to know.

Guiding principles and regulations

All service providers are responsible for any activity carried out under access/account rights assigned to them, whether accessed via The Old Post Office IT equipment or their own device.

No service users should allow any unauthorised person to use The Old Post Office IT facilities and services that have been provided for them.

Service providers should use only their personal logins, account IDs and passwords and not allow them to be used by anyone else.

Screen displays should be kept out of direct view of any third parties when accessing personal, sensitive, confidential or classified information.

Service providers should ensure they log off before moving away from a device during the normal working day to protect any personal, special category, confidential or otherwise classified data and to prevent unauthorised access.

Service providers and users should not introduce or propagate viruses knowingly.

It is imperative that service providers do not access, load, store, post or send from The Old Post Office IT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to The Old Post Office or may bring The Old Post Office into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of The Old Post Office's business activities; sexual comments or images, nudity, racial slurs, sex-specific comments, or anything that would offend someone on the basis of their age, sex, sexual orientation, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or beliefs or disability (in accordance with the Equality Act 2010).

Where necessary, service providers should obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1988. This is particularly relevant when downloading images for use at The Old Post Office.

Service providers Training

New service providers are expected to read The Old Post Office's Online Safety and ICT Acceptable Use Policy, Social Media Policy and the Privacy Policy before starting to provide sessions at the venue.

All service providers have been made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of The Old Post Office community.

All service providers are encouraged to incorporate online safety/e-safety activities and awareness within their curriculum areas.

E-mail

When using email service providers must ensure that they:

● comply with current legislation;

● use email in an acceptable way;

● do not create unnecessary business risk to The Old Post Office by their misuse of the internet.

In addition, service providers should follow the following points on email use:

● When publishing or transmitting information externally, be aware that they are representing The Old Post Office and are seen as speaking on The Old Post Office's behalf. Make it clear when opinions are personal. If in doubt, service providers should speak to Anita Auer;

● Keep electronic files of electronic correspondence, only retaining what is needed.

● If sending personal, sensitive and/or confidential information via email, then the following protocols should be used. If there is any doubt as to the information being sent or the appropriate level of protection required, service providers should check with Anita Auer:

> ○ Personal, sensitive and/or confidential information should be sent securely and any attachment should be encrypted. Service providers should follow the Privacy Policy for further advice on this;

> ○ Any password or key must be sent separately and preferably communicated by another means e.g. telephone or alternative email address;

> ○ Before sending the email, service providers should verify the recipient by checking the address, and if appropriate, telephoning the recipient to check and inform them that the email will be sent;

● Treat others with respect and in a way in which service providers would expect to be treated;

● Do not forward email warnings about viruses. If in doubt, contact Anita Auer for advice.

Do not open an email without a reasonably good expectation of what it contains, and do not download files unless they are from a trusted source. It is the responsibility of each account holder to keep the password secure.

When sending any emails to personal email addresses, for example the email address of a parent, the email address must be entered into the 'Bcc' (blind carbon copy) email address line. Parent or any other personal email addresses must never be entered into the 'To' or 'Cc' of the address line. If emails are being blind copied to more than one parent, no other pupil names or any other personal data should be included in the email. If pupil personal data would be shared with a third party, for example another parent, then separate emails must be sent. All e-mails should be written and checked carefully before sending, including checking attachments. Service providers must inform the DSL if they receive an offensive email.

Use of the internet

Use of the Internet by service providers is permitted and encouraged where such use supports the goals and objectives of The Old Post Office.

However, when using the internet, service providers must ensure that they:

● comply with current legislation;

● use the internet in an acceptable way;

● do not create unnecessary business risk to the organisation by their misuse of the internet.

In particular, the following is deemed unacceptable use or behaviour by service providers and volunteers (this list is non-exhaustive):

● Visiting internet sites that contain obscene, hateful, pornographic or other illegal material;

● Using the device to perpetrate any form of fraud, or software, film or music piracy;

● Using the internet to send offensive or harassing material to other users;

● Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence;

● Hacking, by means of entering or gaining access to a space/account, into unauthorised areas;

● Creating or transmitting defamatory or insulting material;

● Undertaking deliberate activities that waste employee's effort or networked resources;

● Deliberately or recklessly introducing any form of virus into The Old Post Office.

Obscenities/pornography

Service providers must not write, publish, look for, bookmark, access or download material that might be regarded as obscene or pornographic.

Copyright

Service providers should take care to use software legally and in accordance with both the letter and spirit of relevant licensing and copyright agreements. Copying software for use outside these agreements is illegal and may result in criminal charges. Service providers should be aware of copyright law when using content, you have found on other organisations' websites. The law is the same as it is for printed materials. Some digital content is published under Creative Commons (cc) licensing which allows some restricted re-use of said content, service providers should be aware of these restrictions before reusing or adapting the content.

Social Media

Service providers are required to follow this Policy in relation to use of Social Media, including the use of The Old Post Office accounts, and for advice on managing personal social media profiles.

Personal Use

Service providers should ensure that usage is not excessive and does not interfere with work duties. Use should be restricted to non-working hours, unless this forms part of work responsibilities.

Use of facilities for leisure or personal purposes (e.g. sending and receiving personal email, personal phone calls and browsing the internet) is permitted so long as such use does not:

● incur specific expenditure for the The Old Post Office;

● impact on the performance of a member of service provider's job or role

● break the law;

● bring The Old Post Office into disrepute;

● detrimentally affect the network performance by using large amounts of bandwidth (for instance by downloading/streaming of music or videos);

● impact on the availability of resources needed (physical or digital) for business use.

Safe use of Images

Digital images are easy to capture, reproduce and publish and, therefore, misuse. The Privacy Policy must be followed for the storing and use of images of service providers, users, or visitors.

Mobile and personal devices

Service providers must be aware of the Safeguarding Policy and the Behaviour Policy, for service providers obligations in relation to the use of mobiles and personal devices and electronic communication with pupils.

Complaints

Complaints and/or issues relating to online safety/e-safety should be made to the DSL.

Incidents should be logged and The Old Post Office procedure for investigating an online safety/e-safety incident should be followed.

CURRENT LEGISLATION

Acts Relating to Monitoring of Staff eMail

Data Protection Act 2018 http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000 http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998 http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to online safety/e-safety and personal data

● Racial and Religious Hatred Act 2006

● Sexual Offences Act 2003 ● Communications Act 2003 (section 127)

● The Computer Misuse Act 1990 (sections 1 – 3)

● Malicious Communications Act 1988 (section 1)

● Copyright, Design and Patents Act 1988

- Public Order Act 1986 (sections 17 – 29)

- Protection of Children Act 1978 (Section 1)

- Obscene Publications Act 1959 and 1964

- Protection from Harassment Act 1997

- Cloud Computing Services (2014)

- Sexual communication with a child: implementation of s.67 of the Serious Crime Act 2015

Other Policies

We have referred within this document to the following other important policies which should be read in conjunction with this policy:

- Health and Safety Policy
- Risk Assessment Policy
- Privacy Policy
- Safeguarding Policy

This policy is approved and robustly endorsed by The Old Post Office Wellbeing Hub and The Old Post Office C.I.C and is due for renewal every year.

Signed _____*Anita Auer*_____Mrs Anita Auer (Director)

Signed_____*Paul Auer*_____ Mr Paul Auer (Director)

Date: 18.6.24

Review date: 18.6.25

APPENDIX 1: PUPILS' COMPUTER/DEVICE USAGE AGREEMENT – Years R- 4

The named responsible adult (service provider) will ensure they are aware of The Old Post Office's Online Safety and ICT Acceptable Use Policy and Social Media Policy, available on The Old Post Office website.

The named responsible adult will share the following rules with the children. They will sign on the children's behalf to state that the following rules for the use of The Old Post Office IT systems, accounts, equipment/devices are adhered to:

How I use technology at The Old Post Office

I KNOW MY TEACHER WILL:

✓ Use the internet to help me research topics for my work.

✓ Use the internet to make pieces of work look well presented.

I KNOW:

✓ I can ask a service provider if I need help.

✓ I can tell a service providers straight away if I feel worried by anything that I see on the internet or receive in an email or message.

✓ To only send messages that are polite and friendly.

✓ To keep my personal information and passwords safe and not give them out to anyone.

✓ How to look after myself and my friends by using the internet in a safe way.

✓ I understand that I should not use words on the internet or in emails that I would not use in front of a teacher.

✓ I understand that I should not use other people's passwords or login through another person's account.

✓ I understand that online bullying is when a person or a group of people are unkind by using ICT, mobile phones or the internet.

✓ That cyber-bullying will be dealt with as seriously as any real-world bullying incident.

Staying safe

If at any time I feel unsafe using a computer/device then I will talk to a responsible adult straight away.

What I can expect to happen if I do not follow the rules

Appropriate action will be taken in line with The Old Post Office's Behaviour Policy, The Old Post Office's Safeguarding Policy.

On behalf of the children listed, the responsible adult agrees to the Terms and Conditions of the Pupils' Computer/Device Usage Agreement

Signed: …………………………. Print Name: ……………………. Date: ……….

APPENDIX 2: PUPILS' COMPUTER/DEVICE USAGE AGREEMENT – Years 5-8

The Old Post Office's Online Safety and ICT Acceptable Use Policy are available on The Old Post Office website.

This agreement is for the use of The Old Post Office IT systems and The Old Post Office IT (Google) accounts accessed at any time (including during online learning) and equipment/devices and any personal devices (including hand held devices, watches or any other internet enabled device) brought on to The Old Post Office site or at a The Old Post Office activity.

Pupils should also follow any additional code of conduct / guidelines put in place for online learning from home.

How I use technology at The Old Post Office

I DO:

✓ Use internet enabled devices to help me research topics for my work.

✓ Use internet enabled devices to make pieces of work look well presented.

✓ Use internet enabled devices to communicate with service providers if I need to be excused from lessons.

✓ Ask a service provider if I am unsure whether I should be doing something or not or if I need help.

✓ Tell a service provider immediately if I feel uncomfortable or threatened by anything that I see on the internet or receive in an email or message.

✓ Only send emails, messages or any communication that are polite and friendly.

✓ Keep my personal information and passwords safe and will not give them out to anyone.

✓ Know how to look after myself and my friends by using the internet in a safe and responsible way.

✓ Understand that I should not use language on the internet or in emails that I would not use in front of a teacher.

✓ Understand that I should not use other people's passwords; this includes attempting to login through another person's account or accessing another person's files.

✓ Understand that using other people's work and claiming that it is my own is a serious offence.

✓ Understand that any persistent abuse of The Old Post Office IT systems will result in my access being suspended or permanently removed.

✓ Understand that online bullying is when a person or a group of people threaten, tease, embarrass or abuse someone else by using ICT, particularly mobile phones, the internet and related technologies such as social networks.

✓ Know that cyber-bullying will be dealt with as seriously as any real-world bullying incident.

Social Media - for any pupils who access social media

If accessing Social Media sites, pupils should:

● Take responsibility for keeping details of their accounts private, using full privacy settings, logging off properly and not allowing others to use their accounts.

● Report anything offensive or upsetting that they see online to the appropriate bodies, either by using the "report abuse" tabs or by speaking to their parents or a service provider.

● Inform The Old Post Office if they see inappropriate postings by other students, so that steps can be taken to avoid possible repercussions.

Pupils should not:

● Access any social media that is for adults only or if the pupil does not meet the minimum age requirement.

● Access anonymous sites as there is a high risk that inappropriate comments can be exchanged, causing distress or endangerment.

● Include bad, offensive, explicit or abusive language or inappropriate pictures in messages.

● Include anything that could be upsetting, defamatory or insulting towards others or The Old Post Office.

● Regard anything posted online as private. Remember that harassment, defamatory attitudes and racism are just some issues which could lead to prosecution.

It is a serious offence to use another person's account, or to create an account in another person's name without their consent.

Staying safe

If at any time you feel unsafe using a computer/device then find a responsible adult straight away and make sure that your parent is made aware of what is happening.

What you can expect to happen if you do not follow the rules

If the Designated Safeguarding Lead or the service provider consider that there has been a breach of this agreement and/or The Old Post Office rules or there is a safeguarding risk to any individuals, then the DSL or service provider can delegate responsibility for the matter to be investigated and a search to be carried out by the most appropriate individual. This would normally be a parent.

Appropriate action will also be taken in line with The Old Post Office's Behaviour Policy, and The Old Post Office's Safeguarding Policy.

I agree to the Terms and Conditions of the Pupils' Computer/Device Usage Agreement

Signed: …………………………. Print Name: ……………………. Date: ………

APPENDIX 3: PUPILS' COMPUTER/DEVICE USAGE AGREEMENT – SECONDARY AGED CHILDREN / YOUNG PEOPLE

The Old Post Office's Online Safety and ICT Acceptable Use Policy and Social Media Policy are available on The Old Post Office website.

This agreement is for the use of The Old Post Office IT systems and The Old Post Office IT (Google) accounts, accessed at any time (including during online learning) and equipment/devices and any personal devices (including hand held devices, watches or any other internet enabled device) brought on to The Old Post Office site or at a The Old Post Office activity.

Pupils should also follow any additional code of conduct / guidelines put in place for online learning from home. How I use technology at The Old Post Office

I DO:

● Use internet enabled devices to help me research topics for my work.

● Use internet enabled devices to make pieces of work look well presented.

● Use internet enabled devices to communicate with members of service providers if I need to be excused from lessons.

● Ask a service provider if I am unsure whether I should be doing something or not, or if I need help.

● Tell a service provider immediately if I feel uncomfortable or threatened by anything that I see on the internet or receive in an email.

● Only send emails, messages or any communication that are polite and friendly.

● Keep my personal information and passwords safe and will not give them out to anyone.

● Know how to look after myself and my friends by using the internet in a safe and responsible way.

I DO NOT:

● Use language on the internet or in emails that I would not use in front of a teacher.

● Use other people's passwords; this includes attempting to log in through another person's account or accessing another person's files.

● Access inappropriate material such as pornography, gambling websites or anything promoting violence or extremist views.

Use of Social Media

If accessing Social Media sites, pupils should:

● Take responsibility for keeping details of their accounts private, using full privacy settings, logging off properly and not allowing others to use their accounts.

● Report anything offensive or upsetting that they see online to the appropriate bodies, either by using the "report abuse" tabs or by speaking to their parents or a service provider.

● Inform The Old Post Office if they see inappropriate postings by other pupils, so that steps can be taken to avoid possible repercussions.

Pupils should not:

● Access any social media that is for adults only or if the pupil does not meet the minimum age requirement.

● Access anonymous sites as there is a high risk that inappropriate comments can be exchanged, causing distress or endangerment.

● Include bad, offensive, explicit or abusive language or inappropriate pictures in messages.

● Include anything that could be upsetting, defamatory or insulting towards others or The Old Post Office.

● Regard anything posted online as private. Remember that harassment, defamatory attitudes and racism are just some issues which could lead to prosecution.

It is a serious offence to use another person's account, or to create an account in another person's name without their consent.

I UNDERSTAND THAT:

● Using other people's work and claiming that it is my own is a serious offence.

● Any persistent abuse of The Old Post Office IT systems (including The Old Post Office wi-fi) will result in my access being suspended or permanently removed.

● Online bullying is when a person or a group of people threaten, tease, embarrass or abuse someone else by using IT, particularly mobile phones, the internet and related technologies such as social networks.

● Online bullying will be dealt with as seriously as any real world bullying incident.

Staying safe

If at any time you feel unsafe using a computer/device then find a responsible adult straight away and make sure that the Designated Safeguarding Lead or your parents / carers are made aware of what is happening.

What you can expect to happen if you do not follow the rules

 If the Designated Safeguarding Lead, or service provider consider that there has been a breach of this agreement and/or The Old Post Office Rules or there is a safeguarding risk to any individuals, then the DSL or service provider can delegate responsibility for the matter to be investigated and a search to be carried out by the most appropriate individual. This would normally be a parent.

Appropriate action will also be taken in line with The Old Post Office's Behaviour Policy and The Old Post Office's Safeguarding Policy.

Any form of online bullying is regarded as an exceptionally serious offence.

I agree to the Terms and Conditions of the Pupils' Computer/Device Usage Agreement

Signed: ………………………… Print Name: …………………….. Date: ………

APPENDIX 4: SERVICE PROVIDERS COMPUTER / DEVICE AGREEMENT AND CODE OF CONDUCT FOR ICT

To ensure that service providers are fully aware of their professional responsibilities when using IT systems and when communicating with pupils, they are asked to sign this code of conduct. Service providers should consult The Old Post Office's Online Safety and ICT Acceptable Use Policy and Social Media Policy for further information and clarification.

This agreement is for the use of The Old Post Office IT systems, accounts, equipment/devices and any personal devices brought on to The Old Post Office site and used on The Old Post Office network or The Old Post Office activity.

1. I understand that it is a serious offence to use The Old Post Office IT system for a purpose not permitted by its owner.

● I appreciate that IT includes a wide range of systems, including Google accounts, mobile devices, tablets, digital cameras, email, social networking and that this agreement may also include personal IT devices when used for The Old Post Office business

● I understand that The Old Post Office information systems may not be used for private purposes without specific permission from Anita Auer

● I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager

● I will not install any software or hardware without permission

● I will ensure that personal data is stored securely and is used appropriately, whether in The Old Post Office, taken off The Old Post Office premises (with the permission of Anita Auer and encryption approved by the IT department) or accessed remotely

● I will not share any pupil, parent or service provider's personal data with third parties unless there is a lawful reason to do so and/or a third-party agreement is in place

● I will respect copyright and intellectual property rights.

2. I understand that it is my duty to promote online safety/e-safety with service users in my care, to report any matters of concern, and to use electronic communications of any kind in a professional and responsible manner.

● I will promote online safety/e-safety with children in my care and will help them to develop a responsible attitude to system use, communications and publishing

● I will report any incidents of concern regarding children's safety to the Designated Safeguarding Lead and parent / carer

● I will ensure that electronic communications with pupils, including email, are compatible with my professional role and comply with The Old Post Office's Safeguarding Policy.

3. I understand that my use of The Old Post Office information systems, accounts, internet and email may be monitored and recorded to ensure policy compliance.

● I will ensure that I comply with The Old Post Office's Online Safety and ICT Acceptable Use Policy and other relevant policies including the Privacy Policy, and the Safeguarding Policy.

The Old Post Office may exercise its right to monitor and access use of The Old Post Office's information systems, including accounts, devices and internet access, as per the Online Safety and ICT Acceptable Use Policy.

I agree to the Terms and Conditions of the Service providers Computer/ Device Usage Agreement and Code of Conduct for ICT

Signed: …………………………. Print Name: ……………………. Date: ………

SAFEGUARDING STATEMENT

The Old Post Office is committed to maintaining a safe and secure environment for all pupils and a 'culture of vigilance' to safeguard and protect all in its care, and to all aspects of its 'Safeguarding Policy'.

EQUAL OPPORTUNITIES STATEMENT

The aims of The Old Post Office and the principles of excellent pastoral care will be applied to all children irrespective of their race, sex, disability, religion or belief, sexual orientation, gender reassignment or pregnancy or maternity; equally these characteristics will be recognised and respected, and The Old Post Office will aim to provide a positive culture of tolerance, equality and mutual respect.