Use of IT Within School Policy

Author:	Mark Evans
Updated:	September 2021
Review Date:	September 2022
Approved @ Governors:	27/09/2021

Version	Date	Changes
1.0	July 19	Initial version
	May 20	No changes made. Remote learning now covered in additional policy.

Contents

Mobile Phone, Smart Device and Camera Use 5

Introduction 5

Smart Devices & Personal Cameras 5

Staff Policy 5

Use of Devices issued to staff 6

Pupil Policy 7

Parent Policy 8

Social Media Use 8

Introduction 8

Purpose 8

Scope 9

Use of Social Media sites in work time 10

Social Media as part of School Service 10

Social Media applications 10

Guidance/protection for staff on using Social Media 11

Guidance/protection for Pupils on using Social Media 11

Child protection guidance 12

Cyber Bullying 12

Email Acceptable Use 13

Policy Statement 13

Purpose 13

Scope 13

Definition 13

Risks 14

Applying the Policy 15

Internet Acceptable Use 19

Pupil 19

Staff, governor, volunteer, parents and carers 20

School Password Security 20
Introduction 20
Responsibilities 21
Training / Awareness 22
Policy Statements 22
Audit / Monitoring / Reporting / Review 23
Internet Filtering 24
Purpose 24
Inappropriate Material 24
Breaches 24
Requesting Changes to Access 24
Information Security 26
Introduction 26
What do we mean by information? 26
General Principles 27
Scope 29
Rationale 30
Responsibilities 30
Remote Working 30
Purpose 30
Scope 31
Definition 31
Risks 31
Applying the Policy 32
User Responsibility 32
Remote & Mobile Working Arrangements 33
Access Controls 34
Anti-Virus Protection 34
Policy Compliance 34

Smart Device and Camera Use

This section of the policy provides clear guidance on the use of mobile phones, smart devices and digital cameras in school by staff and pupils.

In regard to this policy, a smart device is defined as an electronic device connected to other devices or networks via different wireless protocols such as NFC, Wi-Fi, Cellular connectivity and Bluetooth. This can include, but is not limited to; mobile phones, tablets, smart watches and wearable computers.

Throughout the rest of this policy, all of these products will be referred to as “device” or “devices”.

Introduction

This policy provides guidance on the appropriate use of personal devices by members of staff, pupils and parents.

Old Park Primary School and The Patch Day Nursery has a clear policy on allowing staff and pupils to bring and use mobile phones in school, and this policy makes explicit reference to camera mobile phones.

Smart devices & Personal Cameras

Smart devices are now ubiquitous. A built in digital camera in most of these devices enables users to take high quality pictures. These can then be sent instantly to others using e-mail and social media. They can also be posted on the internet.

There is the potential for these types of devices to be misused in schools. They can become an instrument of bullying or harassment directed against pupils and teachers.

Cameras owned by Old Park and The Patch

Cameras that are owned by the nursery and school only leave the site if required for a trip or event offsite. Cameras are kept in a lockable cupboard and photos are downloaded on a weekly basis and copies are made for display or learning journey evidence. Photographs are then deleted.

Staff Policy

Staff use of personal devices during their working school day should be:

- Outside of their contracted hours
- Discreet and appropriate e.g. Not in the presence of pupils. Staff are asked, if there is a pressing need to use their personal phones during contracted hours, to do so ***only*** in the school staff room.
- Some staff may be asked to carry their device with them at all times in case of emergency. In these cases, staff are asked to continue following the policy regarding use being discreet and

appropriate, and only for emergency use as outlined in the Emergency and Business Continuity Plan.

Devices should be switched off and left in a safe place during lesson times; Most classrooms have lockable cupboards or lockers available in the room, or secure rooms available for staff to access only. School will not take responsibility for items that are lost or stolen.

Staff should never contact pupils or parents from their personal device, or give their personal mobile phone number or online communication platform (such as Twitter or Facebook) details to pupils or parents. If a member of staff needs to make contact with a pupil or parent, a school telephone or online communication platform should be used.

Staff should never send to, or accept from, colleagues or pupils, texts or images that could be viewed as inappropriate.

A member of staff should never use their phone or personal digital camera to photograph a pupil or allow themselves to be photographed by pupils.

This guidance should be seen as a safeguard for members of staff, the school and the Local Authority.

Staff should understand that failure to comply with the policy is likely to result in the enforcement of our Whistleblowing policy and associated procedures.

Use of Cameras and Phones Issued to Staff

Mobile telephones will only be available to staff who have the approval of their Manager, and authorisation of the appropriate member of Senior Leadership. An employee will be eligible to have a mobile phone if it is deemed necessary to their position, and they meet any one of the following criteria:-

- If the employee's duties require them to spend a substantial amount of time out of the office on work related duties (substantial is defined as an average of more than 50% of their working day)
- Staff for whom it is necessary to make essential work related calls off site, as part of their normal course of work
- Staff who are required to be contactable in an emergency situation, when working off-site
- Staff who are on call after normal business hours
- Staff identified through risk assessment procedures

Mobile telephones and cameras issued to staff should be used for work purposes only, unless in exceptional circumstances.

All telephones and cameras should be used in line with the law. Phone calls should not be taken when driving. Drivers should only take calls when the car is correctly parked with the engine off, the car in neutral and the handbrake applied.

Cameras built into mobile telephones should never be used for taking photographs of staff and pupils. Only digital cameras and other devices issued to individuals should be used to take

photographs, videos or audio recordings of pupils. This includes when on educational visits and when filming assemblies and performances. Photographs and videos will also only be taken in accordance with the permissions given by parents at the start of each school year. These are shared with class teachers and discussed with parents if necessary. Explicit permission is also sought from the parents of children involved before sharing any media related to other events e.g. Young voices, residential trips. Any cameras issued for work purposes should be left at a work location, and never taken home.

Equipment issued to staff should be kept secure. PIN number protection (or more complicated password protection where available) must be applied at all times in order to protect the device from improper use. When not in use devices should be stored securely and not left in a location where it could be stolen, such as visible in a car.

Staff when issued with devices will be asked to complete an Issued Equipment Form, which further lays out the expectations placed on staff that are given equipment to use as part of their job role.

Pupil Policy

While we fully acknowledge a parent's right to allow their child to bring a mobile phone to school if they walk to and from school without adult supervision, Old Park Primary School and The Patch Day Nursery discourages pupils from bringing mobile phones to school due to the potential issues outlined above.

When a child needs to bring a phone into school, a permission slip must be signed by their parent and the mobile phone must be left in a secure location within the classroom at the start of the day and collected at the end of the day. Phones should be clearly marked so that each pupil knows their own phone. Parents are advised that Old Park Primary School and The Patch Day Nursery accepts no liability for the loss or damage to mobile phones which are brought into the school or school grounds.

Where a pupil is found by a member of staff to be using a mobile phone, the phone will be confiscated from the pupil and a record will be made of the name of the pupil and attached to the phone. The mobile phone will be stored by a member of SLT or the child's class teacher. The pupil may collect the phone at the end of the school day. A letter will be sent home to the parents requesting that a permission slip be returned the next day. If this practice continues more than three times, then the school will confiscate the phone until an appropriate adult collects the phone from a senior teacher.

If a pupil is found taking photographs or video footage with a mobile phone of either other pupils or teachers, this will be regarded as a serious offence and disciplinary action will be taken according to the school's Behaviour Policy.

If images of other pupils or teachers have been taken, the phone will not be returned to the pupil until the images have been removed by the pupil in the presence of a senior teacher.

Should a pupil be found to be using their phone inappropriately, the school reserves the right to withdraw this privilege and they will no longer be able to bring a phone into school.

Please talk to your child about the appropriate use of text messages as they can often be used to bully pupils.

Should parents need to contact pupils, or vice versa, this should be done following the usual school procedures: via the school office. (tel no. 0121 526 2669)

This policy supports the school's Health and Safety, Anti-bullying, Child Protection, Emergency Planning and Business Continuity and Internet Acceptable Use policies, been endorsed by the Board of Governors, and will be monitored, reviewed and amended as required.

Parent Policy

It is school policy not to allow video or photography by parents at school events. This is shared with parents at the beginning of any event. Any parent seen to be filming or taking photos will be reminded of the expectation and asked to delete the media.

We also ask that any official media from events is not shared on social media platforms. Parents are asked to agree to this before they are able to access any media. Should any media be found on these platforms then we will seek to have it taken down and, if identifiable, will speak to the people found to be sharing it to remind them of their obligations. We may also take action to revoke access to this media or access to media in the future.

Social Media Use

This section of the policy provides clear guidance on the use of and protection of individuals in Old Park Primary School and The Patch Day Nursery who use Social Media.

Introduction

Old Park Primary School and The Patch Day Nursery (hereafter referred to as "The School") is aware and acknowledges the large and increasing number of adults and children that are using social media on the internet, including, but not limited to, some of the widest used Twitter, Facebook and Pinterest.

The widespread availability and use of social media brings opportunities to understand, engage, communicate and share ideas with audiences, peers and colleagues in new ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this use with our reputation.

This policy and associated guidance is to protect members of the school and advise School Leadership on how to deal with potential inappropriate use of social media.

For example, our use of social media has potential implications for our duty to safeguard children, young people and the vulnerable. The policy requirements in this document aim to provide balances to support innovation whilst providing a framework of good practice.

Purpose

The purpose of this policy is to ensure:

- That the school is not exposed to legal risks
- That the reputation of the school is not adversely affected
- That our users are able to clearly distinguish where information provided via Social Media applications is legitimately representative of the school.

Facebook is targeted at older teenagers and adults. They have a no under 13 registration policy and recommend parental guidance for 13 to 16 year olds.

The following are extracts from Facebook privacy policy:

"If you are under age 13, please do not attempt to register for Facebook or provide any personal information about yourself to us. If we learn that we have collected personal information from a child under age 13, we will delete that information as quickly as possible. If you believe that we might have any information from a child under age 13, please contact us"

"We strongly recommend that minors 13 years of age or older ask their parents for permission before sending any information about themselves to anyone over the Internet and we encourage parents to teach their children about safe internet use practices.

Materials to help parents talk to their children about safe internet use can be found on this help page"

This guidance is to advise and protect staff from accusations of improper relationships with pupils:

Scope

This policy covers the use of Social Media applications by all school stakeholders including: employees, Governors and pupils. These groups are referred to collectively as 'school representatives' for brevity.

The requirements of this policy apply to all uses of Social Media applications which are used for any school related purpose and regardless of whether the School representatives are contributing in an official capacity to Social Media applications provided by external organisations.

Social Media applications include, but are not limited to:

Blogs, for example Blogger

Twitter

Online discussion forums, such as netmums.com

Collaborative spaces, such as Facebook

Media sharing services, for example YouTube

All school representatives should bear in mind that information they share through Social Media applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the School's Equality and Diversity Policy.

Use of Social Media sites in work time

Use of Social Media applications in work time for personal use only is not permitted, unless permission has been given by the Head Teacher.

Social Media as part of School Service

All proposals for using Social Media applications as part of a school service (whether they are hosted by the school or by a third party) must be approved by the Head Teacher first

Use of Social Media applications which are not related to any school services (for example, contributing to a wiki provided by a professional association) does not need to be approved by the Head Teacher. However, school representatives must still operate in line with the requirements set out within the policy

School representatives must adhere to the following Terms of Use. The Terms of Use below apply to all uses of Social Media applications by all

school representatives. This includes, but is not limited to, public facing applications such as open discussion forums and internally-facing uses such as project blogs regardless of whether they are hosted on school network or not.

Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct. Old Park Primary School and The Patch Day Nursery expects that users of Social Media applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

Social Media applications

- Must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute. Must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns
- Must not be used in an abusive or hateful manner
- Must not be used for actions that would put school representatives in breach of school codes of conduct or policies relating to staff.
- Must not breach the school's misconduct, equal opportunities or bullying and harassment policies
- Must not be used to discuss or advise any matters relating to school matters, staff, pupils or parents.

- No staff member should have a pupil or former pupil under the age of 18 as a 'friend' to share information with
- Employees should not identify themselves as a representative of the school
- References should not be made to any staff member, pupil, parent or school activity / event unless prior permission has been obtained and agreed with the Head Teacher
- Staff should be aware that if their out-of-work activity causes potential embarrassment for the employer or detrimentally effects the employer's reputation then the employer is entitled to take disciplinary action.
- Violation of this policy will be considered as gross misconduct and can result in disciplinary action being taken against the employee up to and including termination of employment.

Guidance/protection for staff on using Social Media

- No member of staff should interact with any pupil in the school on Social Media sites
- No member of staff should interact with any ex-pupil in the school on Social Media sites who is under the age of 18
- This means that no member of the school staff should request access to a pupil's area on the Social Media site. Neither should they permit the pupil access to the staff members' area e.g. by accepting them as a friend.
- Where family and friends have pupils in school and there are legitimate family links, please inform the Head Teacher in writing.
- It is illegal for an adult to network, giving their age and status as a child
- If you have any evidence of pupils or adults using Social Media sites in the working day, please contact the named Child Protection person in school

Guidance/protection for Pupils on using Social Media

- No pupil under 13 should be accessing Social Media sites. This is the guidance from the United Kingdom Government based upon the age at which a child is considered old enough to consent to passing their personal information to a third party. There is a mechanism on Facebook where pupils can be reported via the Help screen; at the time of time of writing this policy the direct link for this is:

http://www.facebook.com/help/contact.php?show_form=underage

- No pupil may access Social Media sites during the school working day
- All mobile phones must be handed into the Teaching Staff at the beginning of the school day, the Internet capability must be switched off. Failure to follow this guidance will result in a total ban for the student using a mobile phone
- No pupil should attempt to join a staff member's areas on networking sites. If pupils attempt to do this, the member of staff is to inform the Head Teacher. Parents will be informed if this happens
- No school computers are to be used to access Social Media sites at any time of day.
- Any attempts to breach firewalls will result in a ban from using school ICT equipment other than with close supervision

- Please report any improper contact or cyber bullying to you tutor / class teacher in confidence as soon as it happens.
- We have a zero tolerance to cyber bullying

Child protection guidance

If the Head Teacher receives a disclosure that an adult employed by the school is using a Social Media site in an inappropriate manner as detailed above they should:

- Record the disclosure in line with their child protection policy
- Schools must refer the matter to the LA who will investigate via West Midlands Police Child Protection Team.
- If the disclosure has come from a parent, take normal steps to calm the parent and explain processes
- If disclosure comes from a member of staff, try to maintain confidentiality
- The LA will advise whether the member of staff should be suspended pending investigation after contact with the police. It is not recommended that action is taken until advice has been given.
- If disclosure is from a child, follow your normal process in your child protection policy until the police investigation has been carried out

Cyber Bullying

By adopting the recommended no use of Social Media sites on school premises, Old Park Primary School and The Patch Day Nursery protects themselves from accusations of complicity in any cyber bullying through the provision of access.

Parents should be clearly aware of the school's policy of access to Social Media sites.

Where a disclosure of bullying is made, schools now have the duty to investigate and protect, even where the bullying originates outside the school.

This can be a complex area, and these examples might help:

- A child is receiving taunts on Facebook and text from an ex pupil who moved three months ago: This is not a school responsibility, though the school might contact the new school to broker a resolution.
- A child is receiving taunts from peers. It is all at weekends using Facebook. The pupils are in the school: The school has a duty of care to investigate and work with the families, as they attend the school.
- A child is receiving taunts from peers. It is all at weekends using Facebook. The pupils are in Y5: This is the tricky one. The school has a duty of care to investigate and work with the families, as they attend the school. However, they are also fully within their rights to warn all

the parents (including the victim) that they are condoning the use of Facebook outside the terms and conditions of the site and that they are expected to ensure that use of the site stops. At any further referral to the school the school could legitimately say that the victims and perpetrators had failed to follow the school's recommendation. They could then deal with residual bullying in the school, but refuse to deal with the Social Media issues.

- Once disclosure is made, investigation will have to involve the families. This should be dealt with under the school's adopted anti bullying policy.
- If parent / carers refuse to engage and bullying continues, it can be referred to the police as harassment
- This guidance can also apply to text and mobile phone cyber bullying.

Email Acceptable Use

Policy Statement

Old Park Primary School and The Patch Day Nursery will ensure all users of School email facilities are aware of the acceptable use of such facilities.

Purpose

The objective of this Policy is to direct all users of Council email facilities by:

- Providing guidance on expected working practice. Highlighting issues affecting the use of email.
- Informing users about the acceptable use of ICT facilities in relation to emails.
- Describing the standards that users must maintain.
- Stating the actions that may be taken to monitor the effectiveness of this policy.
- Warning users about the consequences of inappropriate use of the email service.

The Policy establishes a framework within which users of Council email facilities can be clear about what is expected of them and their use of email as a communication and recording tool.

Scope

This policy covers all email systems and facilities that are provided by Old Park Primary School and The Patch Day Nursery for the purpose of conducting and supporting official business activity through the Council's network infrastructure and all stand alone and portable computer devices.

This policy is intended for all Old Park Primary School and The Patch Day Nursery employees, governors, partners, contractual third parties and agents of the School who have been designated as authorised users of email facilities.

The use of email facilities will be permitted providing staff have received appropriate training (where applicable) and have confirmed by signing the School's Code of Conduct that they accept and agree to abide by the terms of this policy.

Inappropriate use of email facilities by staff will be regarded as a disciplinary offence.

Definition

All email prepared and sent from Old Park Primary School email addresses or mailboxes, and any non-work email sent using Old Park Primary School ICT facilities is subject to this policy.

Risks

Old Park Primary School and The Patch Day Nursery recognises that there are risks associated with users accessing and handling information in order to conduct official School business.

This policy aims to mitigate the following risks:

- Viruses, malware etc.
- Increased risk of data loss and corresponding fines
- Inappropriate access to and unacceptable use of the Council's network, software, facilities and documents
- Inadequate destruction of data
- The non-reporting of information security incidents
- Inconsistency in how users deal with 'secure' documents
- The impact of insufficient training for users
- The sharing of passwords
- Incorrect or inappropriate classification of documents
- Risk of reputation damage and further loss in public confidence
- Operational difficulties providing services

Non-compliance with this policy could have a significant effect on the efficient operation of the School and may result in financial loss and an inability to provide necessary services to our partners.

Applying the Policy

Email as records

All emails that are used to conduct or support official Old Park Primary School business must be sent using a @oldparkprimary.com address.

Non-work email accounts must not be used to conduct or support official Old Park Primary School business. Members and users must ensure that any emails containing sensitive information must be sent from official school email. All emails that represent aspects of School business or School administrative arrangements are the property of the School and not of any individual employee or partner.

Emails held on School equipment, or equipment provided by third parties on behalf of the School are considered to be part of the schools corporate record and email and email also provides a record of staff activities.

The legal status of email messages is similar to any other form of written communication. Consequently, any e-mail message sent from a facility provided to conduct or support official Old Park Primary School business should be considered to be an official communication from the School. In order to ensure that Old Park Primary School is protected adequately from misuse of email, the following controls will be exercised:

I. All official external e-mail messages will be appended with the following disclaimer

DISCLAIMER
You should be aware that all e-mails received and sent by this School are subject to the Freedom of Information Act 2000 and therefore may be disclosed to a third party. (The information contained in this message or any of its attachments may be privileged and confidential and intended for the exclusive use of the addressee). The views expressed may not be official policy but the personal views of the originator.

- If you are not the addressees any disclosure, reproduction, distribution, other dissemination or use of this communication is strictly prohibited.
- If you received this message in error please return it to the originator and confirm that you have deleted all copies of it.
- All messages sent by Old Park Primary School and The Patch Day Nursery are checked for viruses using the latest antivirus products. This does not guarantee a virus has not been transmitted. Please therefore ensure that you take your own precautions for the detection and eradication of viruses

Whilst respecting the privacy of authorized users, Old Park Primary School maintains its legal right, in accordance with the Regulation of Investigatory Powers Act 200, to monitor and audit the use of email by authorised users to ensure adherence to this Policy. Any such interception or monitoring will be carried out in accordance with provisions of that Act and the School's Conduct and Behaviour Policy. Users should be aware that deletion of email from individual accounts does not necessarily result in the permanent deletion from the School's ICT systems.

It should also be noted that email and attachments may need to be disclosed under the Data Protection Act 1998, the Freedom of Information Act 2000 or GDPR 2018.

Email as a Form of Communication

Email is designed to be an open and transparent method of communication. However, it cannot be guaranteed that a message will be received or read, nor that the content will be understood in the way that the sender of the email originally intended. It is therefore the responsibility of the person sending an email to decide whether an email is the most appropriate method for conveying time critical information or of communicating in the particular circumstances.

Email must not be considered to be any less formal than memos or letters that are sent out from the school. When sending an external email, care should be taken not to contain any material which would reflect poorly on the School's reputation or its relationship with its partners and stakeholders.

Email facilities provided by the School for email should be not used:

- For the transmission of unsolicited commercial or advertising material, chain letters or other junk mail of any kind.
- For the transmission of protected and restricted material concerning stakeholders, partners or the activities of the school, including personal data.
- For the transmission of material that infringes the copyright of another person, including intellectual property rights.
- For activities that unreasonably waste staff effort or use of resources or activities that unreasonably serve to deny service to others.
- For activities that corrupt or destroy other user's data.
- For activities that disrupt the work of other users.
- For the creation or transmission of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images of material.
- For the creation or transmission of any material which is designed or likely to cause annoyance, inconvenience or needless anxiety.
- For the creation or transmission of material that is abusive or threatening to others, or serves to harass or bully others.
- For the creation or transmission of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on the grounds of gender, sexual orientation, marital status, disability, political or religious beliefs.
- For the creation or transmission of defamatory material.
- For the creation or transmission of material that includes false claims of a deceptive nature.
- For the use of impolite terms or language including offensive or condescending terms, also known as flaming.
- For activities that violate the privacy of others.
- For unfairly criticising others, including copy distribution to other individuals.
- For publishing to others the text of messages written on a one-to-one basis, without the prior express consent of the author.
- For the creation or transmission of anonymous messages
- For the creation or transmission of material which brings the School into disrepute.

Junk Mail

Despite junk mail filters being in place, there may be instances where a user will receive unsolicited mass junk email or spam. It is advised that users delete such messages without reading them, or mark the mail as Junk Mail using the built in facilities, to allow the junk mail system to filter future similar messages from being delivered. Do not reply to the email. Even attempting to remove the email address from a distribution list can confirm the existence of an email address following a speculative email.

Before giving your email address to a third party, for instance a website, consider carefully the possible consequences of that address being passed (or possibly sold on) to an unknown third party, and where the benefits outweigh the potential problems.

Chain letter e-mails (those that request you to forward the message to one or more additional recipients who are unknown to the original sender) must not be forward using Old Park Primary School systems or facilities.

Monitoring of email usage

All users should be aware that email usage is monitored and recorded centrally. The monitoring of email (outgoing and incoming) traffic will be undertaken so that Old Park Primary School

- Can plan and manage its resources effectively
- Ensures that users act only in accordance with policies and procedures
- Ensure that standards are maintained
- Can prevent and detect any crime
- Can investigate any unauthorised use

Monitoring of content will only be undertaken by staff specifically authorised for that purpose in accordance with the Communications Policy. These arrangements will be applied to all users and may include checking the contents of email message for the purpose of

- Establishing the existence of facts relevant to the school, partner, supplier and related matters
- Ascertaining or demonstrating standards which ought to be achieved by those using the facilities
- Preventing or detecting any crime
- Investigating or detecting unauthorised use of email facilities
- Ensuring effective operation of email facilities
- Determining if communications are relevant to school business.

Where a manager suspects that a user is abusing email facilities, they should contact the eLearning Manager. This can then be investigated for evidence and audit trails of access to systems. The School will also comply with any legitimate request from authorised bodies under the Regulation of Investigatory Powers legislation for this information.

Access to another employee's email is strictly forbidden unless the employee has given their consent or their email needs to be accessed by their line managed for specific work purposes whilst they are absent. Consent to access the email of another employee must be given by the employee, and any consent must be communicated to the eLearning Manager. Managers must only open emails which are relevant.

Security

Access to emails sent between @oldparkprimary.com addresses is only by 2 factor authentication (key fob and password). However emails that are sent outside this closed network travel over a

public communications network and are liable to interception or loss. There is a risk that copies of email are left within the public communications system. Therefore any private or personal data must not be sent via email outside this immediate network.

Confidentiality

All staff are under a general requirement to maintain the confidentiality of information. There are also particular responsibilities under Data Protection legislation to maintain the confidentiality of personal data. If any member of staff is unsure or whether they should pass on information, they should consult the eLearning Manager.

Staff must make every effort to ensure that the confidentiality of email is appropriately maintained. Staff should be aware that a message is not deleted from the system until all recipients of a message and any forwarded or attached have deleted their copies. Moreover, confidentiality cannot be assured when messages are sent over outside networks, such as the Internet, because of the insecure nature of most such networks and the number of people to whom the messages can be freely circulated without the knowledge of Old Park Primary School.

Care should be taken when addressing all emails, but particularly when they include business sensitive information to prevent accidental transmission to unintended recipients. Particular care should be taken if the email client software auto-completes an email address as the user begins typing a name.

Automatic forwarding of email (for example when the intended recipient is on leave) must be considered carefully to prevent sensitive materials being forwarded inappropriately. Rules can be implemented to include or exclude certain mail based on the sender or subject. If you require assistance with this, please contact a member of SLT in the first instance.

Negligent Virus Transmission

Computer viruses are easily transmitted via email and internet downloads. Full use must therefore be made of Old Park Primary School's anti-virus software. If any user has concerns about possible virus transmission, they must report the concern to the School's outsourced email provider.

In particular users:

- Must not transmit by email any file attachments which they know to be infected with a virus
- Must not download data or programs of any nature from unknown and untrusted sources
- Must ensure that an effective anti-virus system is operating on any computer which they use to access School facilities
- Must not forward virus warnings other than to the School's outsources email providers helpdesk or the eLearning Manager
- Must report any suspected files to a member of SLT

In addition, the School and it's outsourced email provider will ensure that email is virus checked at the network boundary and at the host, and where appropriate will use functionally independent virus checkers.

If a computer virus is transmitted to another organisation the School could be held liable if there has been negligence in allowing the virus to be transmitted. Users must therefore comply with the Software Policy.

Policy Compliance

If any user is found to have breached this policy, they may be subject to Old Park Primary School's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offenders.

If you do not understand the implications of this policy or how it may apply to you, seek advice from a member of SLT.

Internet Acceptable Use

These policies are shared with staff, pupils and parents on a regular basis. We expect them to be signed by staff and members of the governing body. We expect them to be read, discussed and understand by pupils and parents.

Pupil

Foundation Stage and Key Stage 1

I agree that I will:

- Always keep my passwords a secret
- Only open internet pages which my teacher has said are okay
- Only work with people I know in real life
- Tell my teacher or an adult I trust if anything makes me feel scared or uncomfortable
- Make sure all the messages I send are polite
- Show my teacher if I get a nasty message
- Not reply to any nasty message or anything else that makes me uncomfortable
- Not give my mobile phone number, address or any other contact details to anyone who is not a friend in real life
- Only e-mail people I know
- Only use my school e-mail
- 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 and family or pets)
- Not load photos of myself onto the computer

- Never agree to meet a stranger

I understand that anything I do on the computer may be seen by someone else. I understand that if I break the rules, I may not be allowed to use the internet or computers in future.

Key Stage 2

I agree that I will:

Always keep my passwords a secret

- Only visit sites which are appropriate to my learning at the time
- Only work with people I know in real life
- Tell my teacher or an adult I trust if anything makes me feel scared or uncomfortable online
- Make sure all the messages I send are polite
- Show my teacher if I get a nasty message or get sent anything which makes me feel uncomfortable
- Not reply to any nasty message or anything else that makes me uncomfortable
- Not give my mobile phone number, address or any other contact details to anyone who is not a friend in real life
- Only e-mail people I know or those approved by a responsible adult
- Talk to a responsible adult before using anything on the internet including chat rooms or social networking sites
- Keep my personal details private (my name, family information, journey to school, pets and hobbies)
- Always check with a responsible adult and my parents before I show photographs of myself on the internet
- Never meet an online friend without taking a responsible adult that I know with me

I understand that anything I do on the computer may be seen by someone else. I understand that if I break the rules, I may not be allowed to use the internet or computers in future.

Staff, governor, volunteer, parents and carers

ICT technologies are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the school's eSafety coordinator.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.

Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Head teacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature …….…….…… Date ……

Full Name …….....(printed)

School Password Security

Introduction

Old Park Primary School and The Patch Day Nursery will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system

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

Responsibilities

The management of the password security policy will be the responsibility of the Computing Lead, IT technician team and the head and deputy head teacher.

Each class uses a class log-on for logging onto the computers, but will be provided individual passwords for web based services such as their email and learning platforms that the school uses. All other users are provided with individual passwords for all services. All users (adults and young people) will have responsibility for the security of their username and password, and must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Passwords for new users, and replacement passwords for existing users will be allocated by Computing lead and IT technician team.

Adult users of the school's network will change their passwords every 90 days, and cannot be reused within a 900 day period. Password changes on other web based systems will be based upon the default as set by the provider, unless that default can be changed, upon which it will be set to 90 days and no reuse within 900.

Training / Awareness

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. This should apply to even the youngest of users, even if class logons are being used.

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

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

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

- in Computing lessons reinforced during the discussion of online which occurs wherever online safety is relevant and as part of the wellbeing curriculum.
- through the Acceptable Use Agreement

Policy Statements

Users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ELearning Manager (or other person) and will be reviewed, at least annually, by the E-Safety Committee.

All staff users will be provided with a username and password by the computing lead or technician team who will keep an up to date record of users and their usernames. Users will be required to change their password every 90 days.

The following rules apply to the use of passwords: (schools will need to take account of local authority guidance and the level of security required factored against the ease of access required for users)

- passwords for adults must be changed every 90 days (see earlier section under Responsibilities)
- the last ten passwords cannot be re-used
- the password should be a minimum of 6 characters long and
- must include three of – uppercase character, lowercase character, number
- must not include proper names
- the account should be "locked out" following six successive incorrect log-on attempts
- temporary passwords e.g. used with new user accounts or when users have forgotten or need to change their passwords, shall be enforced to change immediately upon the next account log-on
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- requests for password changes should be authenticated by computing lead or technician team to ensure that the new password can only be passed to the genuine user.

The "master / administrator" passwords for the school ICT system, used by the ELearning Manager (or other person) must also be available to the Head teacher or other nominated senior leader and kept in a secure place (eg school safe).

Audit / Monitoring / Reporting / Review

The responsible person will ensure that full records are kept of:

- User Ids and requests for password changes
- User logons
- Security incidents related to this policy

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption.

Local Authority Auditors also have the right of access to passwords for audit investigation purposes

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner.

These records will be reviewed as required.

This policy will be regularly reviewed (preferably annually) in response to changes in guidance and evidence gained from the logs.

Internet Filtering

Policy Statement

Old Park Primary School and The Patch Day Nursery provides Internet connectivity for staff, pupils and visitors via Talk Straight Ltd operating under the name Schools Broadband. The school's filtering facilities are provided by Talk Straight Ltd using the Lightspeed Systems Web Filtering suite of tools.

The Lightspeed Systems filtering software blocks content that has been identified by the international user base of Lightspeed Systems, and automatically filters URLs and websites that are considered inappropriate by the user base. The filters also comply with the Hone Office terrorism block list.

The school also uses desktop level filtering, provided by Future Digital called Future Digital Futures. This allows us to filter at the school level and to fulfil our duties under the UK Government's Prevent Strategy. This software captures any breaches of the school's internet and computer use policy as screenshots to provide evidence of misuse of the school systems, and is applied to all Windows computers owned, managed and operated by the school.

However, any filtering and monitoring services, no matter how thorough can never be completely comprehensive and thus all users access the Internet in accordance with the School's Acceptable Use Policies.

Breaches

If at any time school staff or pupils find themselves able to access Internet sites which they think should be blocked, they should advise a member of SLT immediately, who will arrange to have the content blocked.

Reporting of Inappropriate Content

Where inappropriate material has been accessed via the school network, the person discovering such material will inform the school's Senior Leadership Team. The computing lead or technician team will change the filtering rules accordingly.

In line with the School's Acceptable User Policy parents will be informed when a pupil intentionally accesses inappropriate material.

Where applicable the Head teacher / computing coordinator will inform the Board of Governors and if necessary the Police. Where an incident is likely to involve media interest, the Local Authority and Department for Education should also be informed.

Requesting Changes to access

Where a member of staff wishes to access a website that is currently blocked by the filters, they should request a change to the filter directly to the Computing lead or headteacher, using a provided URL unblock form. The request will then be assessed the site for its suitability to be unblocked. The decision regarding unblocking will then be applied and the requesting user will be informed.

Information Security

Introduction

Information is an important asset and of significant value to Old Park Primary and The Patch Day Nursery. The School must protect its information from threats – internal and external, deliberate or accidental that could disrupt the work of the School or infringe the rights of employees or citizens.

Information Security involves the protection of information for:

Confidentiality	Keeping information out of the wrong hands
Integrity	Making sure information is accurate and complete
Availability	Ensuring reliable and timely availability of information and services

This Policy has been developed using the Sandwell MBC Information Security Policy alongside the internationally recognised standard for information security known as ISO27001. This takes a risk based approach to upholding the 3 key principles as outlined above.

Whilst the aim is to provide facilities for employees to use freely in pursuit of their job, there are however, management and legal issues which must be borne in mind to ensure the effective and appropriate use of information.

Information security protects information from a wide range of threats in order to ensure business continuity, minimise business damage and maximise return on investments and business opportunities.

All information created or processed on behalf Old Park Primary School and The Patch Day Nursery is regarded as being owned and accessible by the School as part of its 'business record'. This Policy focuses on electronic information processed by computer and on protecting the technology used to store, process and transmit it. However the principles apply equally to other forms of information including paper records, microfiche and spoken conversation (including voice mail).

Employees should have no expectation of privacy in anything they create, store, send or receive e.g. internet or email using the School's ICT equipment including any personal use permitted by the School.

The Policy should be read and used in conjunction with all relevant supporting information published on the School's Intranet related to (but not limited to) Information Security and Data Protection.

What do we mean by information?

Information is a generic term used throughout this Policy. It can take many forms e.g. electronic, written or vocal. It would be wrong to assume that information in any form warrants the highest level of protection or may never be disclosed as described in this Policy. Schools, like Central

Government, are being requested to adopt the Government's Protective Marking Scheme which classifies information dependent on its attributes e.g. most people are familiar with the term 'confidential' which is one of the 6 markings available. The Government's protective marking system is designed to help individuals determine, and indicate to others, the levels of protection required to help prevent the compromise of valuable or sensitive assets. The markings signal quickly and unambiguously, the value of an asset and the level of protection it needs.

Therefore in applying this Policy everyone handling information must take a pragmatic and sensible approach e.g. a publically available newspaper or leaflet does not warrant anything near the same protection as an extract from the Child Protection Register and therefore the rules of not keeping it on an unattended desk would be absurd.

Therefore common sense and professional judgement must be applied taking into account other demands such as the Freedom of Information Act. For the avoidance of doubt, other supporting resources and contacts are available as described throughout this Policy.

General Principles

Old Park Primary School and The Patch Day Nursery has a significant investment in ICT and information. The School is dependent on the information it holds and processes. The loss of information or its ICT processing facilities could lead to significant additional costs, loss of revenue and damage to the School's reputation as a result of:

- School activities being fully or partially suspended (if the information is personal data, formal intervention from the Information Commissioner)
- Having to recover information or ICT facilities and equipment
- Unauthorised disclosure of protected information relating to individuals being made available to 'interested parties'
- Vulnerable citizens being put at risk as a result of key information not being available to the people who need it or being disclosed inappropriately
- Fraudulent manipulation of cash or goods

Always remember

- Information security is your personal responsibility. All information will have an owner or author. Know the rules for handling the information in your care. Stick to those rules without exception
- Before making information available to anyone else, make certain you have the authority, including legal power, to release it
- Never access information unless it is part of your job and you have a business need to do so
- Never give out information via the telephone, or in any other way unless you are absolutely sure who you are giving it to, that it is adequately protected whilst in transit and that the recipient is entitled to receive it.
- Remember – always take reasonable and practicable steps to protect the information you store or process

When in the office

- Never leave information out on your desk when you are not present
- Always lock your computer before leaving your desk unattended
- Lock and remove the keys from cabinets or storage units if you leave the office unattended and access to information may be compromised
- Choose your passwords carefully and never let anyone else know them
- Challenge anyone you see in the building who should not be there – do not allow anyone to tail you through any security doors. If they need access to secure doors, they should already have security codes and/or a door fob for electronic access.

On the move

- Never take information out of the office unless you need to. Keep your ICT equipment – laptops, telephones and paperwork secure at all time.
- Never leave equipment, information or documents in an unattended vehicle. Always travel with it locked securely and out of site in a lockable glove compartment or car boot.
- When working in a public place, make sure you are not overheard and that information cannot be seen by others.
- Any data that is moved outside the building, where possible, should be done so via encrypted methods. USB encrypted memory sticks are available to all staff members that are required to be taken data off site, and all laptops that are taken off site should be encrypted before they leave. Staff can also use the provided OneDrive for Business online storage cloud solution. The solution has been configured to not allow for the sharing of data on this with third-party organisations.

Transmitting Information

- Always make sure you know what protective marking the information you are using should have and always comply with that level of protection
- Be certain you are only sending what you absolutely need to and no more
- Ensure the method of transfer is appropriate to the protection of that information and if in any doubt do not use it.
    - Use encryption tools whenever available
- Data Processing Agreements must be in place for any information processed by a third party and the School remains as the recognised Data Processor.

Scope

This Policy defines security standards which apply to all employees, members, contractors, third parties and temporary staff working on behalf of Old Park Primary School and The Patch Day Nursery. It also applies to all agencies, agents or representatives working on behalf of the School and using or processing its information e.g. Children's Centre providers.

This policy is relevant to all information systems whether they be computer or paper based. It covers all devices capable of holding information, the School's entire computer network and also includes information systems not owned by the School but used by employees for School purposes. The includes, but is not limited to information

- Stored on computers
- Transmitted across networks
- Printed out
- Written on paper
- Sent by fax
- Stored on tape, disc, or other electronic means
- Spoken in conversation in person or via telephone/VOIP
- Sent via email, instant message or other electronic communications
- USB flash drives, memory cards or other forms of portable storage (encrypted or otherwise)
- Cloud services, such as but not limited to Microsoft OneDrive, Google Drive, Dropbox

Rationale

Our information security policy is in place to ensure that

- Information owned or processed by the Council is protected against threats, be they internal or external, deliberate or accidental
- Confidentiality of information is assured – we will protect our information from unauthorised access, use, disclosure or interception
- Integrity of information is maintained – we will protect information from unauthorised changes or misuse, so that it can be relied upon as accurate and complete
- Availability – Information is available when and where it is needed
- Legal and regulatory requirements are understood and met
- Information and training on information security is up to date and available to all employees.

Responsibilities

It is everyone's responsibility to make themselves aware of this Policy and adhere to it.

Information security breaches (suspected or definite) should be reported to the Headteacher as soon as is reasonably possible. Do not attempt to cover up any breaches as the consequences for the School and/or the individuals concerned could potentially be much more severe if discovered at a later date.

A formal process exists to record all information security breaches. A formal notification using the appropriate form must be sent to Sandwell Council's Data Protection Officer.

Deliberate breaches of this Policy are regarded as a disciplinary matter. The School reserves the right to take legal action in relation to a serious breach of Policy.

If you do not understand the implications of this policy or how it applies to you, refer to the supporting Codes of Practice and guidance notes or seek advice from a member of SLT.

Remote Working

Old Park Primary School and the Patch Day Nursery (hereafter referred to as 'school') provide users with the facilities and opportunities to work remotely as appropriate to their role. School will ensure that all users who work remotely are aware of the acceptable use of portable computer devices and remote working opportunities.

Purpose

The purpose of this section of the document is to state the Remote Working policy of school. Portable computing devices are provided to assist users to conduct official School business efficiently and effectively. This equipment, and any information stored on portable computing devices, should be recognised as valuable organisational information assets and safeguarded appropriately.

Scope

This document applies to all employees, contractual third parties and agents of the School who use/access Old Park ICT facilities and equipment remotely, or who require remote access to Old Park Information Systems or information.

Definition

This policy should be adhered to at all times whenever any user makes use of portable computing devices.

This policy applies to all users' use of Old Park ICT equipment and personal ICT equipment when working on official School business away from Old Park premises (i.e. working remotely). T

his policy also applies to all users' use of Old Park ICT equipment and personal ICT equipment to access School information systems or information whilst outside the United Kingdom.

Portable computing devices include, but are not restricted to, the following:

- Laptop computers.
- Tablet PCs.
- Mobile phones.

Risks

Old Park recognises that there are risks associated with users accessing and handling information in order to conduct official School business. The mobility, technology and information that make portable computing devices so useful to employees and organisations also make them valuable prizes for thieves. Securing confidential information when users work remotely or beyond the School network is a pressing issue – particularly in relation to the School's need as a data processor to protect data in line with the requirements of the Data Protection Act 1998 and GDPR 2018.

This section aims to mitigate the following risks:

- Increased risk of equipment damage, loss or theft.
- Wider use of mobile IT equipment where personal or sensitive data may be stored.
- Accidental or deliberate overlooking by unauthorised individuals.
- Unauthorised access to confidential information.
- Exposure of personal and sensitive client information.
- Unauthorised introduction of malicious software and viruses.
- Potential sanctions against the School or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse.
- Potential legal action against the School or individuals as a result of information loss or misuse.

- School reputational damage as a result of information loss or misuse.

Non-compliance with this policy could have a significant effect on the efficient operation of the School and may result in financial loss and an inability to provide necessary services to our customers, as well as exposing sensitive and/or personal client data to unauthorised users/environments.

Applying the Policy

All ICT equipment (including portable computer devices) supplied to users is the property of Old Park It must be returned upon the request of Old Park. Access for the ICT Technician of Old Park shall be given to allow essential maintenance, security work or removal upon request. All ICT equipment will be supplied and installed by the Old Park ICT Technicians . Hardware and software must only be installed following approval by Old Park. Users who wish to install any hardware or software must contact the Business Manager before this is carried out.

User Responsibility

It is the user's responsibility to ensure that the following points are adhered to at all times:

a) Users must take due care and attention of portable computer devices when moving between home and another business site.

b) Users will not install any hardware to or inside any School owned portable computer device, unless authorised by Old Park Business Manager. Users will allow the installation and maintenance of Old Park installed Anti Virus updates immediately.

c) Users will inform the Business Manager of any School owned portable computer device message relating to configuration changes.

d) Business critical data should be stored on the school server wherever possible and not held on the portable computer device. Confidential information should be saved in the staff private folder and not in shared folders.

e) All mobile devices (e.g. laptops and tablet PC's) must be locked with a password/PIN number.

f) Personal, sensitive or confidential documents can only be stored on either a school issued encrypted USB drive, on an encrypted school issued laptop or within an appropriately permissioned folder on Google Drive.

g) Personal or sensitive documents must not be viewed or downloaded on mobile devices.

h) If you take a school laptop home with you, it should be stored in a secure location and you must make sure that it is not left in your car etc.

i) All faults must be reported to the IT Technician immediately.

j) Users must not remove or deface any asset registration number and only those devices with an asset number/tag can be connected to the School network.

k) User requests for upgrades of hardware or software must be approved by the Business Manager. Equipment and software will then be purchased and installed by ICT Technician if appropriate.

l) Personal use of the ICT equipment by staff is allowed outside of working hours. However this policy and acceptable use must be fully adhered to. In particular, the equipment must not be used in relation to running an external business and websites containing illegal, unsuitable and inappropriate material, must not be accessed. Only software approved by Old Park can be used (e.g. Word, Excel, Adobe, etc.). The ICT equipment is supplied for the employee's sole use and nobody else, including family members, must use it.

m) The user must ensure that reasonable care is taken of the ICT equipment supplied. Where any fault in the equipment has been caused by the user, in breach of the above paragraphs, Old Park may recover the costs of repair (calculated at a pre-determined rate). This charge is subject to annual review.

n) The user should seek advice from the Headteacher before taking any School supplied ICT equipment outside the United Kingdom. The equipment may not be covered by the School's normal insurance against loss or theft and the equipment is liable to be confiscated by Airport Security personnel.

o) Old Park may at any time, and without notice, request a software or hardware audit, and may be required to remove any equipment at the time of the audit for further inspection. All users must co-operate fully with any such audit.

p) Any user who chooses to undertake work at home or remotely in relation to their official duties using their own IT equipment must understand that they are not permitted to hold any database, or carry out any processing of confidential information relating to the School, its employees, or pupils/parents. Under no circumstances should personal or confidential information be emailed to a private non-School email address.

Remote and Mobile Working Arrangements

Users should be aware of the physical security dangers and risks associated with working within any remote office or mobile working location.

Equipment should not be left where it would attract the interests of the opportunist thief. In the home it should also be located out of sight of the casual visitor. For home working it is recommended that where possible the office area of the house should be kept separate from the rest of the house. Equipment must be secured whenever it is not in use, e.g. put away in cupboard, locked in cabinet etc.

Users must ensure that passwords are kept in a separate location to the portable computer device at all times. All removable media devices and paper documentation must also not be stored with the

portable computer device. Passwords and/or other access information should not be written down and stored near the portable device.

Paper documents are vulnerable to theft if left accessible to unauthorised people. These should be securely locked away in suitable facilities (e.g. secure filing cabinets) when not in use. Documents should be collected from printers as soon as they are produced and not left where they can be casually read. Where personal and sensitive information is being printed on shared printers extreme care should be taken to ensure all documents are collected from the printer and that interruptions to printing due to paper jams, empty paper trays etc do not lead to sensitive documents being discovered by unauthorised staff.

Waste paper containing confidential information must be shredded to required standards. If paper documents containing sensitive information are taken outside the office, the number of documents/cases should be limited in the same was as electronic records.

Access Controls

It is essential that access to all confidential information is controlled. This can be done through physical controls, such as locking the home office or locking the computer's keyboard. Alternatively, or in addition, this can be done logically such as by password controls or User Login controls.

Portable computer devices should be switched off, logged off, or the keyboard locked when left unattended, even if only for a few minutes.

All data on portable computer devices must be encrypted. If this is not possible, then all confidential data held on the portable device must be encrypted. It is School policy to encrypt/lock all laptops.

Remote users' access to School systems (if connecting over public networks, such as the Internet) will need to be via a secure route. No other access routes can be used.

The user shall ensure that appropriate security measures are taken to stop unauthorized access to confidential information, either on the portable computer device or in printed format.

Users are bound by the same requirements on confidentiality and Data Protection as Old Park itself.

Anti Virus Protection

Users who work remotely must ensure that their portable computer devices are connected to the corporate network at least once every week (unless valid reasons why this cannot be achieved, e.g. sickness/holiday) to enable the Anti Virus software to be updated.

Policy Compliance

If any user is found to have breached this policy, they may be subject to Old Park's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from the Headteacher or a member of the SLT.