Boorley Park School

Initial Policy:	May 2019
Policy Updated:	May 2021
Next Review:	May 2022
Key Person:	TLS

Information Communication Technology (ICT) Policy

Mission Statement

The school is committed to the use of ICT across the curriculum and to providing all pupils, staff and members of the Boorley Park Primary School community with access to the technology which will enhance teaching, facilitate learning and prepare them for the technological demands of a rapidly changing world.

Principles

- To raise educational standards across all areas of the curriculum.
- To ensure staff, pupil, parent and Governor training in the use of ICT is of the highest standard.
- To provide access on demand to technology that will meet the statutory demands and requirements of the National Curriculum in all subject areas.
- To offer equal opportunities in ICT to all members of the school and allow access to ICT to the local community if applicable.
- To ensure that all members of the school community understand E-safety (see policy).
- To ensure that all members of the school community understand Data Protection (see policy).

Practice

Curriculum

- The curriculum will ensure that all pupils will:
  - Leave the school computer literate.
  - Be autonomous users of ICT.
  - Be able to make full use of the opportunities for research, analysis and communication afforded by Information Communication Technology.
  - Develop computational thinking skills.
  - Be curious and creative in their use of ICT to solve problems and answer questions.

- It will equip all our pupils with the necessary skills and modes of thinking so that they will succeed in a constantly changing society, where a high level of skill in the use of new technologies can be the currency for employment.
- It will not be seen as a separate subject in its own right, but as a powerful tool to enhance, engage, motivate the teaching and learning in all areas of the curriculum. It is to be used by all subject areas as an integrated part of each pupil's education.

ICT and Computing will be taught across the curriculum and wherever possible, integrated into other subjects. There may be a need for stand-alone ICT and/or Computing sessions to teach skills that can then be applied in the cross-curricular sessions. The long term ICT and Computing map will show the journey in which the children are expected to take but this will be adapted each year to ensure that it is relevant and up-to-date. The ICT leader will ensure that the plans provide coverage of the National Curriculum and that children are challenged and are able to succeed.

Early Years

It is important in the foundation stage to give children a broad, play-based experience of ICT in a range of contexts, including outdoor play. ICT is not just about computers. Early Years learning environments should feature ICT scenarios based on experience in the real world, such as in role play. Children gain confidence, control and language skills through opportunities to 'paint' on the whiteboard or drive a remote-controlled toy. Outdoor exploration is an important aspect, supported by ICT toys such as metal detectors, controllable traffic lights and walkie-talkie sets. Recording

devices can support children to develop their communication skills. This is particularly useful with children who have English as an additional language.

By the end of key stage 1 pupils should be taught to: -

- understand what algorithms are, how they are implemented as programs on digital devices, and that programs execute by following a sequence of instructions;
- write and test simple programs;
- use logical reasoning to predict and computing the behaviour of simple programs;
- organise, store, manipulate and retrieve data in a range of digital formats;
- Communicate safely and respectfully online, keeping personal information private, and recognise common uses of information technology beyond school.

By the end of key stage 2 pupils should be taught to:

- design and write programs that accomplish specific goals, including controlling or simulating physical systems;
- solve problems by decomposing them into smaller parts;
- use sequence, selection, and repetition in programs; work with variables and various forms of input and output; generate appropriate inputs and predicted outputs to test programs;
- use logical reasoning to explain how a simple algorithm works and to detect and correct errors in algorithms and programs;
- understand computer networks including the internet; how they can provide multiple services, such as the world-wide web; and the opportunities they offer for communication and collaboration;
- describe how internet search engines find and store data; use search engines effectively; be discerning in evaluating digital content; respect individuals and intellectual property; use technology responsibly, securely and safely;
- Select, use and combine a variety of software (including internet services) on a range of digital devices to accomplish given goals, including collecting, analysing, evaluating and presenting data and information.

Assessment

Teachers regularly assess capability through observations and looking at completed work. Key objectives to be assessed are taken from the national curriculum to assess key ICT and Computing skills each term. Assessment is process orientated - reviewing the way that techniques and skills are applied purposefully to tasks by pupils to demonstrate their understanding of the concepts of ICT and computing. Pupils are closely involved in this process.

Assessment can be broken down into;

- Formative assessments that are carried out during and following short focused tasks and activities. They provide pupils and teaching staff the opportunity to reflect on their learning in the context of the agreed success criteria. This feeds into planning for the next lesson or activity.
- Summative assessment should review pupils' capability and provide a best fit view through the use of independent open ended assessment tasks that provide opportunities for pupils to demonstrate capability in relation to the term's work. There should be an opportunity for pupil review and identification of next steps. Summative assessment should be recorded for all pupils – showing whether the pupils have met, exceeded or not achieved the learning objectives.

We assess the children's work in ICT and computing by making informal judgements as we observe the children during lessons. We mark each piece of work against the lesson objective- using the school marking and feedback guidelines. Once the children complete an end of unit assessment task, we make a summary judgement of the work for each pupil as to whether they are working towards, meeting or exceeding the expectations of the unit. We record the results and we use these to plan future work, to provide the basis for assessing the progress of the child and to pass information on to the next teacher at the end of the year. ICT and Computing work is saved on the school network. Other work may be printed and filed within the subject from which the task was set.

Resources

- Dedicated computer equipment is available within the school. This is matched to the requirements of the curriculum and the age/ability of pupils using it.
- All rooms have access to the Internet, either via hardwired network ports or the school-wide wireless network.
- Every classroom from Early Years to Y6 has an interactive screen with sound and DVD facilities.
- Boorley Park Primary School maintains a suite of software that covers the typical mainstream uses of ICT, for example, word processing, spreadsheet and presentations on the most popular operating systems. We also maintain a suite of software that caters for more specialist use appropriate to specific subjects.
- Each pupil has a unique identity with corresponding storage space and access to the various school online platforms.

System Security

- Virus protection is installed and updated regularly.
- School ICT system security will be reviewed regularly.
- The downloading or installation of executable files in any form is expressly forbidden.
- Filtering: The School will use a filtering system that is a DfE approved provider and work with the IWF (Internet Watch Foundation) to maintain lists of keywords for blocking. Includes terrorism/extremism/intolerance categories.

Responsibilities –

The Headteacher and other members of the Senior Leadership Team (SLT) are responsible for:

- Monitoring the teaching of ICT and Computing throughout the school.
- Deciding on the provision and allocation of resources throughout the school in accordance to the School Development Plan, ICT action plans and timescales
- Ensuring that the ICT leader and teachers are following their roles as listed below and in accordance to job specifications and performance management targets.

The ICT and Computing Leader is responsible for:

- Producing an ICT and Computing development plan and for the implementation of the ICT and Computing policy across the school.
- Offering help and support to all members of staff (including Learning Support Assistants) in their teaching, planning and assessment of ICT and Computing.
- Maintaining resources and advise staff on the use of software and hardware
- Monitoring classroom teaching or planning following the schools rolling programme of monitoring.
- Monitoring the children's ICT and Computing work, looking at samples of different abilities.
- Leading staff training on new initiatives.
- Attending appropriate training and keeping staff up to date with relevant information and developments.
- Having enthusiasm for ICT and Computing and encouraging staff to share this enthusiasm.
- Keeping parents and governors informed on the implementation and developments of ICT and computing in the school.
- Liaising with all members of staff on how to reach end of year expectations
- Helping staff to use assessment to inform future planning.

Class teachers are responsible for:

- Ensuring that pupils in their classes have opportunities for learning ICT and Computing skills and using ICT and Computing across the curriculum
- Monitoring and recording pupil progress in computing.
- Responding to, and reporting, and e-safety or cyber bullying issues that they encounter within or out of school in accordance to e-safety procedures (see e-safety policy)
- Following and agreeing to, the Acceptable Usage Agreement (see appendix 2 and appendix 5).

- Securing motivation, concentration and enthusiasm for ICT and Computing

Pupils with Special Educational Needs or Disabilities (see also SEND policy)
We believe that all pupils have the right to access ICT and Computing. In order to ensure that pupils with Special Educational Needs achieve to the best of their ability, it may be necessary to adapt the delivery of the ICT and Computing curriculum for some pupils. We teach ICT and Computing to all pupils, whatever their ability. Through the teaching of ICT and Computing we provide learning opportunities that enable all pupils to make progress. We do this by setting suitable learning challenges and responding to each child's different needs. Where appropriate ICT and computing can be used to support pupils with SEND on a one to one basis where pupil receive additional support. Additionally, as part of our dyslexia friendly approach to teaching and learning we will use adapted resources wherever possible such as visual timetables, different coloured backgrounds and screen printouts.

Equal Opportunities and Inclusion
Boorley Park Primary School will ensure that all pupils are provided with the same learning opportunities regardless of social class, gender, culture, race, disability or learning difficulties. As a result, we hope to enable all pupils to develop positive attitudes towards others. All pupils have equal access to ICT and computing and all staff members follow the equal opportunities policy. Resources for pupils with SEND and disadvantaged pupils will be made available to support and challenge appropriately.

Linked Policies : Anti-Bullying Policy
British Value Statement
Child Protection Policy
Complaints Policy
Code of Conduct for Staff
Data Protection Policy
E-Safety Policy
Publication Schemes (FOI) Policy
Preventing Radicalisation and Extremism
Safeguarding Policy
Whistleblowing (Protected Disclosures) Policy

Appendix 1
Cyber Security Checklist 2019

1. Home and mobile working

Is there a clear policy on mobile working, with all associated training?
All Wildern Academy Trust staff are provided with a handbook for all the schools procedures and rules. Staff also visit a training session on using IT safely when starting at Wildern Academy Trust. This is run by one of the senior members of the IT Support Staff.

Is a secure baseline build applied to all devices?
All devices owned by Wildern Academy Trust are imaged with software containing all the latest operating system security and anti-virus updates.

Is data protected outside formal work environments, including in transit?
All staff laptops are password protected. All members of SLT, DoPAs and DoLs have their laptops encrypted also. USB Drives are all Encrypted & All sensitive email attachments are password protected.

2. User education and awareness

Does the trust have security policies covering acceptable and secure use of systems?
The Wildern Academy Trust utilises all forms of security on our systems this ranges from Active Directory security groups to limit access to sensitive data, Group Policies designed to restrict usage of settings & potentially harmful extensions and a staff acceptable use policy which must be signed by all new staff members.

Is there a staff training programme covering secure use of systems, including awareness of cyber risks – for example strengthening passwords, risk from public wifi hotspots, risks from use of removable media such as USB sticks, avoiding use of personal accounts for business purposes, and maintaining backups?
All Wildern Academy Trust staff are provided with a handbook for all the schools procedures and rules. Staff also visit a training session on using IT safely when starting at Wildern Academy Trust. This is run by one of the senior members of the IT Support Staff. Every Year there is a staff meeting on eSafety and Data Protection.

Do staff know how to report issues and incidents?
During new starter training and at regular staff training, staff are told to ensure all issues are reported to ithelp@wildern.org or for Data breaches to report them to dataprotection@wildern.org

3. Incident management

Does the trust have an incident response and disaster recovery capability, with suitably trained staff?
Mission-critical backups are taken on a nightly basis which can be used in a disaster recovery scenario. These backups are stored on an off-site server in a colocation centre located 20 minutes down the M27. Access to this server needs to be approved by either the IT Manager or IT Systems Manager. If a disaster recovery scenario was activated, the IT Manager would handle logistical issues, and the IT Systems manager would handle recovery of mission-critical data and setup of new systems using this data. Both the IT Manager and IT Systems Manager are trained and have experience in creating a whole network and domain from scratch. All trust data is uploaded monthly to an archive in the cloud with a secure third party so that in the event of a major disaster all data for Virtual Machines and File Store Data is recoverable.

Are there incident management plans and are these tested?
The only tested part of the incident management plan is the physical movement of the colocation server from the hosting centre in Fareham to Wildern. Once at Wildern the server was brought online and integrated with our network.

Are criminal incidents reported to law enforcement bodies?
Yes. Any criminal behaviour that is caught on the Wildern Academy Trust network is first isolated and reported to the IT Manager who will then conduct an investigation. The findings of this investigation are then passed to SLT and on to the police.

4. Information risk management regime
Is there a governance structure for managing information risk?
The Academy Trust has a clear line of governance via the IT Manager, Assistant Headteacher and then IT Trustee.

Do information professionals liaise with central government, stakeholders and suppliers to understand the threat?
Yes at all levels connections are made via various associations, memberships, Hampshire County Council and DfE updates.

Does senior management understand and engage with risk mitigation processes?
The IT Assistant Headteacher updates the Headteacher regularly and other members of the Senior team as required.

5. Managing user privileges
Are there effective account management processes, with limits on privileged accounts?
The Wildern Multi Academy Trust utilises Active Directory security groups to limit access to sensitive data to Group Policies designed to restrict usage of settings & potentially harmful extensions.

Are use privileges controlled and monitored?
All users within our domain are correctly placed into groups suitable for their role within the organisation. This is regularly checked and correct information gathered before increasing a users security privileges.

Is access to activity and audit logs controlled? Are these logs reviewed for unusual behaviour?
All activity and audit logs are controlled by members of the IT Support team and are regularly reviewed for unusual behaviour as well as alerts & notifications being set up for key phrases and actions.

6. Removable media controls
Is there a policy on the use of removable media (eg CDs, flash/pen drives, mobile phones, wireless printers)?
All removable media is scanned for malicious content before linking to the system all removable media is encrypted to ensure sensitive data is kept secure. Mobile phones are joined to the WiFi using a PPSK this means we can track a user's location and browsing history on mobile devices as well as monitoring for malicious content. Wireless printing is managed through Papercut which is a printer management software which allows us full control over all printing and printer settings & preferences.

Are media scanned for malicious software (malware) before being linked to the system?
Our Antivirus is designed to scan all media for malicious content before linking it to the system.

7. Monitoring
Is there a monitoring strategy in place for all ICT systems and networks?
All internet traffic for the Wildern Academy Trust is passed through our Smoothwall S14 Appliance this monitors all browsing traffic for malicious or unsuitable content. The Wildern Academy Trust will be looking to implement Solarwinds or similar to monitor and report on all switch and server infrastructure in line with the new schools.

Do logs and other monitoring activities enable the identification of unusual activity that could indicate an attack?
All Smoothwall logs are processed with the username of the browser. This means we are able to take the appropriate action going forward. The Wildern Academy Trust will be looking to take steps in the right direction with Intrusion detection & switch monitoring using Solarwinds or similar.

8. Secure configuration
Does a system inventory exist?
All new hardware and software is recording in our Inventory Spreadsheet.

Are security patches applied regularly?
Critical security patches are pushed out for all windows operating systems via our SCCM server.

Is there a minimum defined baseline for all devices?
All devices owned by Wildern Multi Academy Trust are imaged with an image containing all the latest operating system security updates and antivirus.

9. Malware protection
Are there effective anti-malware defences in place across all business areas?
All Wildern Multi Academy Trust devices are installed with the latest security updates and Antivirus with the latest definitions.

Is there regular scanning for malware?
All Wildern Multi Academy Trust device run regularly scheduled malware scans.

What changes have been made as a result of monitoring results?
Multiple changes have been made since monitoring results these include; Encryption of USB sticks, disabling certain file extensions from being run by unauthorised users, encryption of senior staff laptops and more documentation on using the school network safely.

10. Network security
Is the network perimeter managed?
The Wildern Multi Academy Trust utilises a Juniper SRX340 as a Firewall & entry point to the Wildern network this provides protection from malicious content and actions.

Do information professionals understand where the highest risk information assets are and how they are protected?
The Wildern IT Support Team are regularly trained and information constantly updated on Wikis for all security and network infrastructure. This means the team have a good knowledge of the protocols and protections on high risk assets.

Are security controls monitored and tested?
All security controls are controlled by members of the IT Support team and are regularly reviewed for unusual behaviour as well as alerts & notifications being set up.

Appendix 2
Internet Access

- The Computer Misuse Act 1990 provides penalties for unauthorised access to computer material, including finding or attempting to guess someone's password. This is an offence even if no damage is done. Further penalties are provided if unauthorised access is gained with intent to commit further offences such as fraud or theft. In addition the unauthorised modification of computer material, including deleting someone else's files, changing the desktop setup or introducing viruses to a computer system with intent to impair the operation of the system carries heavy penalties.

- The benefits to pupils from Internet access, in the form of information and resources from across the world and opportunities for collaboration and communication, exceed any disadvantages.
- Internet use is part of the statutory curriculum and is a necessary learning tool for staff and pupils.
- Internet access will be an integral part of schemes of work to enrich and extend learning activities.
- Our School provides a filtering system in line with LA requirements which restricts access to inappropriate material.
- The Internet Access Policy has been written by ICT staff within the Wildern Academy Trust and will be reviewed on an annual basis.
- Parents will be provided with information about the School's supervised, monitored and filtered Internet access arrangements. A copy of the Acceptable Use Policy will be printed and posted near all computers in the School.
- Internet access will be withdrawn from use if required contrary to the Acceptable Use Policy.
- Pupils will be educated in taking responsibility for Internet access and appropriate use of the Internet and digital communications. They will be supervised at all times when they are using the Internet and every reasonable precaution will be taken to protect pupils from accessing undesirable material.
- Pupils will be educated in the effective use of the Internet including skills of research, knowledge location and evaluation as well as how to validate information and to observe copyright.

Appendix 3
Email

- E-mail is an essential means of communication within education and care should be taken to compose e-mail messages as formal communications.
- Governors have been provided with a school email address and this should be used for all school communication.
- Staff should not use their personal or school email addresses to communicate with parents. All messages should be sent to a member of SLT who will then approve them to be sent from a central 'admin' email address.
- Responsible and appropriate use within the school will be encouraged for all our users, (staff, pupils and wider community such as parents) and messages sent from a school computer or using the school domain name will be regarded in the same way as messages written on school headed paper.
- Mailing lists, blogs and other social networking activities will only be available to our users for supervised and/or specific purposes.
- Users may only use approved Boorley Park Primary e-mail accounts on the school system. All members of staff and pupils are provided with this account on arrival at Boorley Park Primary.
- Communication with staff should be only used for school related reasons.
- Users must report if they receive an offensive email.
- Incoming email should be treated as suspicious and attachments not opened unless the author is known.
- Users should be educated in the responsible use of communications via email and electronic means and not to share personal details.
- Users should understand that the appropriate use of the school computer network maintains good order, which means not only preventing illegal or undesirable behaviour, but also ensuring that the use of shared facilities such as a computer or a network is neither jeopardised nor disrupted.
- All our users should be aware that the school reserves the right to inspect and electronically filter e-mails and their contents. Any misuse of e-mails will result in disciplinary sanctions.

Appendix 4
Social networking

Staff should demonstrate awareness of their role as a significant figure in the lives of children and young people, lead by example, and model the characteristics they are trying to inspire in young

people. They should recognise the important role of the school in the life of the local community, and take responsibility for upholding its reputation and building trust and confidence in it.

In practice, this means that members of staff at the school should not be interacting with pupils within a closed, or semi-closed environment. Online interaction within an 'open' online environment may be appropriate, but depends on the context and requires professional judgement. If in doubt, staff should consult their line manager for advice.

- 'Closed' communications: Instant messaging, personal email, direct messages, etc.
- 'Semi-closed' communications: Writing on a 'wall' within Facebook, communicating with someone who 'protects' their updates on Twitter, etc.
- 'Open' communications: Blog comments, standard Twitter updates, wikis, etc.

Communications with pupils should be appropriate to the staff professional remit. For the majority of pupils this will mean discussing only academic work with them. Such boundaries will inevitably be different when contact relates to extra-curricular activities, but staff should remember that family friendships and networks outside of school should not prejudice or affect school-based activities. Apart from the obvious e-safety implications of social networks, pupils expect and have a right to be treated equitably by members of staff. Contact via social networking sites potentially prejudices this.

The entire community of Boorley Park Primary users including staff, pupils, parents and Governors are expected to model appropriate behaviour. As a Rights and Respecting School users recognise our engagement through social networking will be responsible and not malign members of our school community. It is advised that any ‘groups’ and online communities joined/accessed, such as Facebook or Twitter, can be seen and should not reflect negatively on staff professionally and/or Boorley Park Primary School.

Appendix 5
Boorley Park Primary School Acceptable Use Policy (AUP)

This policy explains the behaviours, which are acceptable and unacceptable, with regard to usage of the School’s network.

- Any person using Boorley Park Primary School’s Network or Service is required to comply with this Acceptable Use Policy. A summary version of this document must be signed by all users of the school network to show that they agree to abide by this AUP. Failure or non-compliance may result in the School denying that person access to the school network.
- This Acceptable Use Policy has been endorsed and approved by the Board of School Governors.
- The School seeks to promote high standards of teaching and learning by supporting the effective use of ICT.
- This policy applies to all users of the Boorley Park Primary School network this includes local authority officers, headteachers, Governors, teachers, pupils, classroom assistants, parents, voluntary helpers, school caretakers and other auxiliary staff.
- All users should note that the Boorley Park Primary School network is monitored on a regular basis, and that Boorley Park Primary School reserve the right to delete anything held on their network and remove access rights without prior warning.
- Any user who is found to deliberately infringe this policy may be subject to disciplinary procedures or legal action.

The Boorley Park Primary School Network and associated services may be used for lawful purposes only. As a user of this Service you agree not to use the Service to send or receive materials or data, which is:

- In violation of any law or regulation.
- Defamatory, offensive, abusive, indecent, obscene.
- Deemed harassment.
- In breach of confidence, privacy, trade secrets.

- In breach of any third party Intellectual Property rights (including copyright).
- In breach of any other rights or has any fraudulent purpose of effect.

You are also prohibited from storing, distributing, transmitting or permitting the storage distribution or transmission (whether intentionally or otherwise) of any unlawful material through the service.

Unlawful and Illegal Use

All material which depicts the abuse of children and young people is illegal. Other illegal material includes race hatred, terrorism and incitement to violence. These are not exclusive categories. There may be other information/material that is deemed to be illegal.

Accidental access to material, which may be classed as illegal should be reported to the Schools Network Manager & Internet Watch Foundation – www.iwf.org.uk.

Any User of the Boorley Park Primary School Network who accidentally comes across illegal material should do the following:

1. Report the incident to the Headteacher or Network Manager or a senior member of staff who should then report to the Network Manager.
2. Do not show anyone the content or make public the URL.
3. Make sure a reference is made of the incident in a log-book.
4. Go to the IWF website at www.iwf.gov.uk and click the report button.

Inappropriate Use
Please be aware that the use of ICT during the time specified as your school work day should be restricted to educational purposes. Personal use of equipment and resources should be restricted to outside of these times.

Inappropriate use of the network includes accessing or having possession of material that is thought to be offensive such as, adult pornography of any level, content of an obscene, indecent and/or abusive nature.

You should be aware that disciplinary and/or civil action might arise if users are found to be accessing material of this nature across the School, Local Authority or regional network.

Security and Protection
All users of the Boorley Park Primary School network will be individually identifiable. This means that every user of the network will have an individual username and password. This must be securely kept and not passed onto other users.

In the event of an investigation into misuse, proper use of passwords will protect innocent users from the upset and embarrassment of suspicion for inappropriate or illegal misuse.

Members of staff who have rights to the school network should take care to ensure that no unauthorised user obtains access to their password. This includes accidental or deliberate access by leaving machines active when not in use by authorised personnel. Any user of the Boorley Park Primary School network who feels their password may have been compromised should contact the Network Manager and request a password reset.

Appendix 6
Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the Internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the Internet. Such images may provide avenues for

cyberbullying to take place. Digital images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out Internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images online.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect every-one's privacy and in some cases protection, these images should not be published online unless consent has previously been given.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Users must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

Appendix 7
Data Protection

The primary purpose of current data protection legislation is to protect individuals against possible misuse of information about them held by others. Under the provisions of the Data Protection Act 1984, specific legislation was introduced in relation to automated data. The impact of the legislation has been considerably widened under the terms of the Data Protection Act 1998 which came into force on 1 March 2000 and (referred to in the General Data Protection Regulation (GDPR). Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website.

The Act regulates the holding and processing of personal data, that is information relating to living individuals, which is held either on computer or in some cases in manual form.

The Act provides individuals with rights in connection with personal data held about them. It provides individuals with the right to access data concerning themselves. It also includes the right to seek compensation through the courts from damages and distress suffered by reason of inaccuracy or the unauthorised destruction or wrongful disclosure of data.

All staff or other individuals who have access to, or use, personal data have a responsibility to exercise care in the treatment of data and to ensure that such information is not disclosed to any unauthorised person. Examples of data include address lists and contact details as well as individual files. Any processing of such information must be done in accordance with the principles outlined above.

One effect of the new eighth principle, which restricts the transfer of material outside the European Economic Area is that personal data about an individual placed on the world wide web is likely to breach the provisions of the Act unless the individual whose data is used has given his or her consent.

The GDPR establishes six principles as well as a number of additional duties that must be adhered to at all times:

1. Personal data shall be processed lawfully, fairly and in a transparent manner

2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (subject to exceptions for specific archiving purposes)

3. Personal data shall be adequate, relevant and limited to what is necessary to the purposes for which they are processed and not excessive;

4. Personal data shall be accurate and where necessary, kept up to date;

5. Personal data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

6. Personal data shall be processed in a manner that ensures appropriate security of the personal

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

There is stronger legal protection for more sensitive information, such as:

- Ethnic background.
- Political opinions.
- Religious beliefs.
- Health.
- Sexual health.
- Criminal records.

GUIDANCE FROM THE INFORMATION COMMISSIONER'S OFFICE RECOMMENDS:

Basis for Processing

The Act requires that there should always be a legitimate basis for the processing of personal data. The Commissioner accepts that the publication of examination results takes place on the basis of a condition described in paragraph 6 of Schedule 2 of the Act. Namely where "the processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason or prejudice to the rights or freedoms or legitimate interests of the data subject".

Information to be provided to pupils and parents

The Act also makes it clear that in order for the processing of personal data, including its collection, to be fair, it is necessary to ensure that those to whom the data relate are aware of the purposes for which their data may be used or disclosed. While it is likely that many pupils and parents will be aware that examination results may be published this is not always the case. To satisfy this requirement therefore, the school should ensure that pupils and their parents are made aware that examination results may be published and in what form.

The right to object

Although the Commissioner does not think that pupils or their parents must give their consent to the publication of examination results, experience shows that in a small number of cases publication can cause distress. When informing pupils or their parents that examination results are published, the school should therefore advise them of the right to object to publication.

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 01625 545 745 or 0303 123 1113 (local rate)

Disclaimer

Boorley Park Primary School will endeavour, wherever possible, to provide a safe and secure environment for its users. However, users must be aware that we cannot guarantee complete safety from inappropriate or illegal material.