Data Protection, Access to Information, Computer Security and Archiving Policy (including EYFS)

This policy reflects GEMS current guidelines and practice. GEMS is not liable for any error in print or otherwise
Contents

Rationale 3
Linked Policies and Cross References 3
Aims 3
Interpretation 3
The Data Protection Act 3
Responsibilities 4
Data Processing 5
Use of Digital Images 9
Computer Security 10
Copyright and Licences 12
Annex 1: Document retention schedules 15
Annex 2: Computer Security Legislation 17
Annex 3: CCTV Check List 19

Date of most recent registration with ICO 16 January 2016
Named Data Protection Officer Ashley Scammell
Data Protection, Access to Information, Computer Security and Archiving Policy

Rationale: Schools are required to process and store data in accordance with the Data Protection Act 1998 (DPA) and to publish information to parents as required by the Department for Education (DFE) and the Independent Schools Inspectorate (ISI).

Linked Policies and Cross References: GEMS Values; Admissions, Attendance and Registration Policy; Assessment, Marking, Recording and Reporting Policy; Behaviour Policy; Information and Communications Technology Policy; Social Media Policy; Child Welfare and Safeguarding Policy; Employee Handbook; Disaster Recovery Plans; Copyright, Designs & Patents Act 1988; The Computer Misuse Act, 1990; The Data Protection Act 1998; Subject Access Code of Practice (ICO 2013).

Points of contact: UK IT Manager; Regional Director of Schools; Director of HR.

Aims

- To ensure that school procedures, record keeping and the handling of personal data comply with the DPA;
- To ensure compliance with copyright licensing laws;
- To provide guidelines to staff regarding the rights of parents to access information we hold about their child(ren);
- To make staff aware of how we handle their personal data; to publish information to parents on school websites as required by the DFE and the Independent Schools Inspectorate (ISI).

Interpretation

References to "parents" in this Policy includes a reference to all those with parental responsibility for a pupil.

References to a “pupil” include past, current or prospective pupils.

The Data Protection Act

Schools gather, hold and process information on both pupils and staff and in doing so, must follow the requirements of the DPA. The DPA covers the collection, storing, editing, retrieving, disclosure, archiving and destruction of personal data. The Act applies to data held on paper as well as electronically. For example - it applies to teacher records/mark books.
“Personal data” means recorded information we hold about our staff, parents or pupils from which they can be identified. It may include contact details, other personal information, photographs, and expressions of opinion about the individual or indications as to our intentions about them.

"Processing" means doing anything with the data, such as accessing, disclosing, destroying or using the data in any way.

It is important that all staff are very careful about the information they record as the DPA gives individuals the right of access (subject to certain exceptions) to information held by the School about themselves.

Each school in the GEMS group registers with the Information Commissioner every 12 months. In this school the person with responsibility for making this registration is the UK IT Manager.

The following link takes you to the relevant page for the latest application form: -

http://www.ico.org.uk/for_organisations/data_protection/registration

The DPA sets out 8 data protection principles that must be adhered to regarding personal data. These say all personal data held must be:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Not kept longer than necessary;
- Processed in accordance with the individual’s rights;
- Secure; and
- Not transferred to people or organisations situated in countries without adequate protection.

Under the DPA an individual can claim compensation from a data controller (school) for damage and distress caused by any breach of the Act.

Responsibilities

The head teacher is responsible for:

- ensuring that staff are provided with a copy of this policy and that it is explained at induction and during staff refresher courses;
- ensuring that the school is registered with the Information Commissioner under the DPA;
• appointing a data protection officer (named at the front of this policy) to ensure that all personal data is processed in compliance with this policy and the DPA;

• ensuring that the following are published on the school website in line with regulatory requirements:
  - child welfare and safeguarding policy;
  - policy for preventing bullying (usually annex to behaviour policy);
  - the complaints procedure and the number of complaints registered under the formal procedure during the preceding school year.

**Data Processing**

Processing will usually only be carried out where one of the following conditions has been met:

• the individual has given his or her consent. In the case of a pupil, consent may be given by the pupil's parents unless the child is of an age to give consent for themselves. Children aged 12 and over may be able to give consent but consideration must be given to each individual case as to whether, in the School's reasonable opinion, the child has sufficient maturity and understanding to give consent;

• the processing is necessary for the performance of a contract with the individual;

• the processing is required to comply with a legal obligation;

• the processing is necessary to protect the vital interests of the individual;

• the processing is necessary to carry out public functions;

• the processing is necessary in order to pursue the School's legitimate interests or the legitimate interests of third parties.

“Sensitive personal data” (racial or ethnic origin; political opinions; religious or similar beliefs; trade union membership; health; sex life; criminal proceedings or convictions) will only be processed if:

• the explicit consent, in writing, of the individual is obtained; or

• the processing is required by law for employment purposes or the administration of justice or legal proceedings; or

• the processing is required for the protection of the vital interests of the individual or a third party.
How we are likely to use your personal data

We will process data about staff for legal, personnel, administrative and management purposes and to enable us to meet our legal obligations as an employer, for example to pay staff, monitor their performance and to confer benefits in connection with their employment.

We will process data about pupils and parents for legal, academic, administrative and management purposes and to enable us to meet our legal obligations to pupils as a provider of education to them.

We may process sensitive personal data relating to staff including, as appropriate:

- information about an employee's physical or mental health or condition in order to monitor sick leave and take decisions as to the employee’s fitness for work;
- the employee's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
- in order to comply with legal requirements and obligations to third parties.

We may process sensitive personal data relating to pupils and parents, including as appropriate:

- information about a pupil's physical or mental health or condition in order to monitor attendance and academic progress and take decisions with regard to the pupil's educational or pastoral needs;
- in order to comply with legal requirements and obligations to third parties.

Processing for limited purposes

We will only process personal data for the specific purpose or purposes notified to staff, pupils and parents or for any other purposes specifically permitted by the DPA.

Adequate, relevant and non-excessive processing

Your personal data will only be processed to the extent that it is necessary for the specific purposes notified to you.

Accurate data

We will keep the personal data we store about you accurate and up to date. Data that is inaccurate or out of date will be destroyed. Please notify us if your personal details change or if you become aware of any inaccuracies in the personal data we hold about you.
The head teacher is responsible for ensuring that files are checked annually to ensure that the information stored is accurate and relevant. Parents will be asked to update the details held by the school on a regular basis. No private written records are to be kept by a member of staff.

**Data retention**

We will not keep your personal data for longer than is necessary for the purpose. This means that data will be destroyed or erased from our systems when it is no longer required. For guidance on how long certain data is likely to be kept before being destroyed please see Annex 1: Archiving schedules.

The records of pupils moving to another school will be hand-delivered to the new school by a member of staff (not parents) or posted directly to the destination school using recorded delivery. If transferred electronically data will be sent via a secure connection to the other school.

**Processing in line with your rights**

Staff, pupils and parents have the right to:

- request access to any personal data we hold about them;
- prevent the processing of their data for direct-marketing purposes;
- ask to have inaccurate data held about them amended;
- prevent processing that is likely to cause unwarranted substantial damage or distress to them or anyone else; and
- object to any decision that significantly affects them being taken solely by a computer or other automated process.

**Data security**

We will ensure that appropriate measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

We have in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. We will only transfer personal data to a third party if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

Maintaining data security means guaranteeing the confidentiality, integrity and availability (for authorised purposes) of the personal data.

Staff files are stored in a locked cabinet in the HR Office. Pupil files are kept in Prep School and Senior School respectively. Access to staff files/records is restricted to the head teacher and HR Manager and authorised GEMS personnel.
The Capita SIMS Management Information System is used to store pupil and staff data. Access to data is monitored and controlled through the allocation of specific access profiles to each member of staff using the system.

Staff data are also held within a proprietary payroll system for the purposes of processing the monthly payroll. Access to this system is restricted to those staff authorised to enter and update the information required for the accurate maintenance of the payroll.

Providing information to third parties

We will not disclose your personal data to a third party without your consent unless we are satisfied that they are legally entitled to the data and we have verified their identity. Where we do disclose your personal data to a third party, we will have regard to the eight data protection principles.

Subject access requests

If you wish to know what personal data we hold about you, you must make the request in writing, with an accompanying fee of £10. All such written requests should be forwarded to the head teacher.

We may ask you to verify your identity by producing your passport or photocard driving licence and green counterpart. If the request is in relation to the personal data of a pupil we may seek evidence that you have parental responsibility for the pupil.

If a child makes a request to access their personal data we will consider whether the child is of an age to be able to understand the meaning of making such a request. Children aged 12 or over may have sufficient understanding but each case will be decided according to the individual child.

The school will not comply with requests by pupils that personal data are not disclosed to parents/guardians unless the school believes disclosure of the information is likely to put the pupil in danger or cause damage or distress. In such cases, the head teacher must consult with GEMS Director of HR.

If you wish to inspect the personal data you may do so in situ in the presence of the head teacher or a person nominated by the head teacher. If you require copies of the personal data we shall provide these to you subject as set out below. We have 40 days from receipt of the request and the fee to comply with your request.

The data set out below is exempt from the right of access under the DPA:

- information which identifies other individuals. However, we will, where reasonably possible redact from the personal data information which identifies other individuals and supply the information to you;

- information which the school believes is likely to cause damage or distress; and
• information to which the legal profession has privileged rights.

The school will also have regard to the following when considering what other information (if any) to withhold:

• information that might cause serious harm to the physical or mental health of the pupil or another individual;

• information that would reveal that the child was at risk of abuse, where disclosure of that information would not be in the child’s best interests;

• information contained in adoption and parental order records; and

• certain information given to a court in proceedings concerning the child.

Breaches of this policy

If you consider that this policy has not been followed in respect of personal data about you or others you should raise the matter with the head teacher. Any breach of this policy will be taken seriously. If a breach involves a member of staff it may result in disciplinary action.

Use of Digital Images

For the purposes of this section, “publication” includes on websites, in the press, on TV, as web broadcasts or video/CD/DVD to be released into the public domain.

• Consent from parents to photographs of their children being taken and/or published is deemed to be given in accordance with clause 10 (e) of the terms and conditions of the contract with parents unless the parent informs the Headteacher in writing and also advises their child that their photograph is not to be taken or published and tells the child to raise the matter at the time. When a parent does not agree to their child’s photograph being used, the Headteacher must inform staff and staff must make every effort to comply.

• The naming of published images of pupils should be avoided wherever possible. This includes photographs, videos, TV presentations, web pages, and press releases. Where it is preferred that named images are used specific written permission from the parent must be obtained.

• Where possible, the school will avoid publishing the full names of students in printed or published material. There may be specific cases where the use of full names is justified at the Head teacher's discretion (e.g. Speech Day program; examination schedules).

• Schools should be aware that the recording of images of children participating in extra-curricular events that are taken for personal use
is not prohibited by the Data Protection Act. These include uses such as parents taking photographs of sports day or videoing a school nativity. Schools should monitor the use of cameras and anyone behaving inappropriately at extra-curricular events. If there are concerns the headteacher can require the person to cease using the camera or leave the premises. The photograph or video should ideally focus on the activity. Where possible images should be recorded of pupils in small groups.

- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate for material published by the School.

- The copyright in all material commissioned by the School should be owned by the School, and where this is not the case, the School must obtain the permission of the copyright owner to reproduce the material and the published material should then be attributed to the copyright owner.

Refer to the school Welfare and Safeguarding Policy for further guidance on the use of mobile telephones and cameras by pupils and staff on school premises and on school transport.

**Computer Security**

The head teacher is responsible for ensuring that:

- school procedures comply with the Data Protection Act;
- only licensed software is used;
- access controls are set with appropriate levels of security;
- passwords are used by only one person, changed regularly, and not disclosed to another person;
- computer use is legitimate and that staff are aware of their responsibilities and security levels for data access;
- only authorised terminals are connected to the network system and that these are logged off immediately after use, or locked if being left unattended;
- access rights are cancelled as soon as staff leave;
- information is secured against loss or corruption; and
- waste computer output (printouts, CDs etc.) are immediately disposed of in a secure manner.

As a result of increasing reliance on computer-based systems, the security and confidentiality of information is extremely important. Some computer crimes are now criminal offences and prison sentences can be imposed. A
manager may be charged as well as the person committing the crime. See Annex 2: Computer Security Legislation.

Computer data requires different levels of security and access, depending upon the degree of confidentiality. Some data are intended for easy use and access is not restricted. However, all data needs to be secured against loss or corruption.

Sensitive and confidential data e.g. pupil files, budgets, that is to be transferred via a mobile data device must be transferred in an encrypted format. Once the transfer to an appropriate and secure system has taken place the file can be safely deleted from the mobile data device, and unencrypted on the new system. Care must be taken that the mobile data device is not lost or carelessly mislaid. If the mobile data device is lost or mislaid then it must be reported to the UK IT Manager.

Passwords must be changed on a regular basis, as determined by the E-Safety Committee.

**Computer Equipment**

All computer equipment must be adequately protected against theft, malicious damage or unreasonable environmental surroundings. Access devices such as keys, card keys, passwords or codes must not be transferred to another person. Computer equipment is not insured if:

- Taken from an unattended vehicle that is not securely locked;
- Left visible in a locked vehicle;
- Taken abroad on a non-work based visit; and
- Not in the possession of a duly authorised representative of GEMS.

The physical security of each piece of computer equipment in a school is the responsibility of the senior staff and ICT co-ordinators and in head office the responsibility of the individual user.

Wherever possible, administration terminals should be placed in positions that only allow the screen’s display to be seen by authorised staff. Consideration should be given to the use of specially designed filters to be placed over computer screens to limit visibility by others.

All confidential output must be stored securely when not in use.

**Backups**

Copies of computer files are taken by the IT team regularly from the servers (the frequency to be determined for each application), and users files are synchronised to the network each time that they log on to the network. For machines that are not connecting regularly or never to a network then an external backup device must be used for this purpose. Copies must be stored securely away from the computer in an encrypted format.
Recovery procedures for all important systems must be specified in each school’s Disaster Recovery Plan. They should be reviewed and tested periodically to ensure that they are still workable.

**Privacy**

Every effort must be made to ensure that confidential information can only be accessed by persons who have permission to see it.

**Intellectual Rights**

Unauthorised copies of licensed software must not be made. GEMS may fund and facilitate the development of software that enhances the professional standing and status of the company. In such instances, a contract will be drawn-up specifying remuneration and copyright.

**Copyright and Licences**

Copyright is an unregistered right (unlike patents, registered designs or trade marks). Therefore, there is no official action to take (no application to make, forms to fill in or fees to pay). Copyright comes into effect immediately, as soon as something that can be protected is created and "fixed" in some way, such as on paper, on film, via sound recording, or as an electronic record on the internet. Copyright work should be marked with the copyright symbol © followed by your name and the date, to warn others against copying it, but it this not legally necessary in the UK.

The head teacher is responsible for ensuring that the necessary copyright licenses are obtained in school as follows:
## Data Protection and Access to Information Policy – last modified 20.04.16 (hbs)

<table>
<thead>
<tr>
<th>Activity</th>
<th>CLA</th>
<th>ERA</th>
<th>PPL</th>
<th>PRS</th>
<th>MCPS</th>
<th>CCLI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reproducing of hymns and worship songs.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>School play, concert, live or recorded music.</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Radio or television broadcast for educational purposes.</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Photocopying articles from journals, magazines or books.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Playing radio/CD/tape in administration offices or staffroom.</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>School disco, fete or fair outside school hours where music played.</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Overhead transparencies from journals, magazines or books.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hiring premises for keep fit/aerobics.</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>After school film/video club.</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Music on hold on telephone system.</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Creating or storing school's computer system the school's own hymn book or carol sheets.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Video or audio recordings of school carol service or other religious/seasonal festival to circulate to parents.</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Recording school concert, play other event containing music.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

### Key to agency abbreviations:

**CLA** – The Copyright Licensing Agency Ltd licenses the photocopying of extracts from books, journals and magazines.

**ERA** – The Educational Recording Agency Ltd. licenses designated educational establishments to record radio and television broadcasts for non-commercial educational purposes.

**PPL** – represents the UK record industry, licensing the use of sound recording (CDs, tapes, discs etc.) on behalf of record companies and performers. Licenses are issued for extra curricular use of copyright sound recordings on school premises.

**PRS** – is the copyright collection society for composers and publishers of music. It licenses the extra curricular use of copyright music on school premises, including PA events and use by hirers.

**MCPS** – represents its composer and publisher members, whenever a musical work is recorded on a CD, tape, video or DVD or when the recording is issued to the public. This applies to the recording of school concerts, plays or other events.
CCLI – Christian Copyright Licensing (Europe) Ltd is the UK’s major licensing body for the reproduction of hymns and songs used during assemblies. CCLI can license schools to reproduce the lyrics and music of many thousands of songs: written; stored on computer; photocopied; acetate sheets.

**Academic pupil records and accident forms must be kept for 3 years.** The records of pupils moving to another school must be taken by school staff (not parents) or posted directly to the destination school using recorded delivery.

The documents must be stored in separate containers with the date clearly written on the outside. **Examination results and child protection information must not be destroyed.**
Annex 1: Document retention schedules

**Employment Records**

The School will retain Employment records to meet the school’s business needs in line with the schedule below before data is securely destroyed. A list is maintained of the file name or identifier for all records destroyed and the date on which this action was taken.

<table>
<thead>
<tr>
<th>Nature of Record</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recruitment records</td>
<td>9 months from completion of recruitment process</td>
</tr>
<tr>
<td></td>
<td>Applications may be held on file for longer than 9 months in case another suitable vacancy arises.</td>
</tr>
<tr>
<td></td>
<td>If so, the applicant should be advised and agreement obtained.</td>
</tr>
<tr>
<td>Vetting records</td>
<td>12 months</td>
</tr>
<tr>
<td></td>
<td>Records which contain sensitive personal data should be destroyed within this period but a note of</td>
</tr>
<tr>
<td></td>
<td>the fact the check has been undertaken and the result whether satisfactory/unsatisfactory can be</td>
</tr>
<tr>
<td></td>
<td>retained until employment ends.</td>
</tr>
<tr>
<td>Criminal convictions</td>
<td>12 months or if retained beyond that period, when conviction is spent in accordance with Rehabilitation of Offenders Act</td>
</tr>
<tr>
<td></td>
<td>This is sensitive personal data which should be destroyed within the period shown unless it is</td>
</tr>
<tr>
<td></td>
<td>relevant for employment purposes.</td>
</tr>
<tr>
<td>General employment records (application form, CV, references, personal details,</td>
<td>Review 12 months after employment ends and destroy personal data no longer required.</td>
</tr>
<tr>
<td>absence records, bank account details, disciplinary records)</td>
<td>Otherwise destroy 6 years from date employment ends.</td>
</tr>
<tr>
<td>Employment information relevant to pension (e.g. role, salary information and</td>
<td>Destroy 12 years from date employment ends</td>
</tr>
<tr>
<td>payroll data, dates of employment)</td>
<td></td>
</tr>
<tr>
<td>Sickness/injury records, medical information other than injuries sustained at</td>
<td>12 months after employment ends.</td>
</tr>
<tr>
<td>work</td>
<td></td>
</tr>
<tr>
<td>Injuries sustained at work</td>
<td>3 years after date of accident.</td>
</tr>
</tbody>
</table>
Pupil Records

The School will retain pupil records in line with the schedule below to meet business needs before data are securely destroyed. A list is maintained of the file name or identifier for all records destroyed and the date on which this action was taken.

<table>
<thead>
<tr>
<th>Nature of Record</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration Form</td>
<td>Review 12 months after pupil leaves the School and destroy personal data</td>
</tr>
<tr>
<td>Parents’ lifestyle or financial information</td>
<td>(including sensitive personal data) no longer required. Otherwise, destroy 2 years</td>
</tr>
<tr>
<td>Pupil attendance records</td>
<td>after the pupil has left the School</td>
</tr>
<tr>
<td>Medical information/sickness absence records</td>
<td>Review 12 months after pupil leaves the School and destroy personal data</td>
</tr>
<tr>
<td>Reports re: special educational needs or learning disabilities</td>
<td>(including sensitive personal data) no longer required. Otherwise, destroy 2 years</td>
</tr>
<tr>
<td>Records relating to educational matters – progress reports; academic achievements;</td>
<td>A copy of the student’s records should be</td>
</tr>
<tr>
<td>correspondence from teachers; information from parents and/or pupils, references</td>
<td>held in archive storage until the student is</td>
</tr>
<tr>
<td>received from other schools</td>
<td>25 years old.</td>
</tr>
<tr>
<td>Child protection records</td>
<td>Indefinitely – in confidential filing.</td>
</tr>
<tr>
<td>Information relating to an accident suffered at School or whilst under the</td>
<td>3 years.</td>
</tr>
<tr>
<td>supervision of the School</td>
<td></td>
</tr>
</tbody>
</table>
Annex 2: Computer Security Legislation

Copyright, Designs & Patents Act 1988

This Act makes it a criminal offence carrying a maximum sentence of two years imprisonment for managers to distribute, or let staff distribute, illegal copies of software within their organisation.

All software being used within departments must have adequate software licences. Packages run on hard disc machines must have their own individual copy. Sufficient copies of software discs must be purchased so that copies are used on only one machine at any given time. However, one disc/CD ROM can be licensed for multiple users.

Copyright in a work is infringed by a person who without licence of the copyright owner does, or authorises another to do, any of the acts restricted by the copyright.

If any person fails to comply with any direction given under this Act or makes or causes to be made an application for the registration of a design in contravention of that section, s/he shall be guilty of an offence and liable to conviction and imprisonment.

The Computer Misuse Act, 1990

This act details three new offences:

- unauthorised access including “hacking” or eavesdropping where the contents of computer files are modified;

- ulterior intent whereby legal power includes both the use of a computer to commit an offence and also, where it aids the committing of another offence;

- unauthorised modification whereby an offence is committed if any action by the offender causes unauthorised modification of the contents of a computer with the intention of disrupting or damaging its contents.

Unauthorized Access (Hacking)

Examples of offences:

- deliberately attempting to access a computer knowing that you are not allowed such access; this applies to just switching on a computer without authority to use it;
- trying out a list of passwords – an offence is committed as soon as the computer shows an error message;
- using telephone networks to search computer lines.
**Ulterior Intent (Hacking with intent to commit a serious crime)**

This is deliberately attempting to access a computer without authority but with the intention to commit a serious crime. This offence is much more serious than unauthorised access, and to be proved it is necessary to show:

- there was a deliberate access to a computer;
- they had no authority to do so;
- they knew they were not authorised;
- there was an intention of using the information to commit a further offence.

The penalties are severe: five years imprisonment (or more) and an unlimited fine.

**Unauthorised Modification (Destruction or alteration of programs or data)**

This is intentionally and without authorisation destroying or altering data or programs. This covers viruses, worms, logic bombs, Trojan horses etc. A person is guilty of this offence if:

- s/he does any act which causes an unauthorised modification of the contents of any computer;
- at the time he does the act he has the requisite intent and the requisite knowledge.

The requisite intent is an intent to cause modification to the contents of any computer and by so doing:

- impair the operation of any computer;
- prevent or hinder access to any program or data on any computer;
- impair the operation of any such program or the reliability of such data.

The penalties for this are an unlimited fine and up to five years imprisonment.

In all of the above the burden of proof will fall on an organisation’s electronic records of access and consequently security procedures will be open to scrutiny.
Annex 3: CCTV

Introduction
The purpose of this Policy is to regulate the management, operation and use of the closed circuit television (CCTV) system at Sherfield School. The system comprises a number of fixed cameras located within and around the school buildings. All cameras are controlled from the Facility Manager’s Office and the system can only be accessed by nominated Senior Management Team or the Facilities’ Manager.

The school owns the internal CCTV system.

The Policy will be subject to regular review by the Senior Management Team, to include consultation as appropriate with interested parties.

This Policy follows the Data Protection Act guidelines.

Objectives of the CCTV Policy

The objectives of Sherfield School’s use of CCTV are:

a) To increase personal safety of students, staff and visitors, and reduce the fear of crime
b) To protect the school buildings and their assets
c) To support the Police in a bid to deter and detect crime
d) To assist in identifying, apprehending and potentially prosecuting offenders
e) To protect members of the public and private property
f) To assist in managing the school

Statement of intent

This CCTV equipment and the images recorded by it are controlled by the Facilities Manager who is responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose (this is a legal requirement of the Data Protection Act 1998). The Facilities and Operational Team and Senior Management Team have considered the need for using a CCTV system and has decided it is required in line with the objectives above.

Cameras will be used to monitor activities within the school and the grounds to identify adverse activity actually occurring, anticipated or perceived, and for the purpose of securing the safety and well being of the schools students and staff, together with its visitors.

At no time will a camera be directed to follow or track an individual.

Cameras are not placed in view of changing areas or toilet cubicles and/or urinals but may be placed in corridors adjacent to the toilets or changing rooms.
Materials or knowledge secured as a result of CCTV use will not be used for any commercial purpose. Copies of footage will only be released to the SMT to investigate misconduct. Images will never be released to the media for purposes of entertainment.

The planning and design has endeavoured to ensure that the CCTV Scheme will give maximum effectiveness and efficiency within available means, but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Warning signs, as required by the Code of Practice of the Information Commissioner, have been placed at all access routes to areas covered by the school’s CCTV system.

**Operation of the system**
The CCTV system will be administered and managed by the Facilities and Operational Management Team in accordance with the values and objectives expressed in the code.

The CCTV system may be operated 24 hours each day, every day of the year, recording all activity at the discretion of the Facilities Manager and Head Master.

Recorded data will be retained no longer than is necessary. In the normal course of events images will be retained for up to 30 days (50 days if over the school holiday) and will then be overwritten. If images are required beyond this period a copy will be taken and stored securely in line with the procedures set out below. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

**Control and Liaison**
The school will periodically check and confirm the efficiency of the system and, in particular, that the equipment is properly recording and that cameras are functional. Senior management will liaise with suppliers regarding servicing and/or repairs and maintenance of the system. Senior management will aid in meetings between interested parties where the provision of CCTV footage is required.

**Monitoring procedures**
Camera surveillance may be maintained at all times and footage continuously recorded and held on system memory. Where it is deemed necessary to retain images for longer than 30 days, the data will either be transferred to a portable storage medium or will be saved on a hard drive accessible to the Facilities and Operational Management Team and Senior Management only in a password protected and uniquely referenced folder.
To maintain and preserve the integrity of any portable storage media used to record events from the hard drive and the facility to use them in any future proceedings, the Facilities Manager adheres to strict procedures of use and retention.

_Breaches of the policy (including breaches of security)_
The Facilities and Operational Management Team and Head Master, or senior manager acting on their behalf, will initially investigate any breach of the CCTV policy by school staff. Any serious breach of the policy will be subject to the terms of disciplinary procedures already in place.

_Putting policy into Practice_
The Headmaster and Facilities and Operational Management Team may carry out performance monitoring, including random operating checks.

_Complaints_
Any complaints about the school’s CCTV system should be addressed to the Deputy Head (The Data Protection Officer). Complaints will be investigated in accordance with the school’s Complaints Policy.

_Access by the Data Subject_
The Data Protection Act provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about them, including those obtained by CCTV. Requests for Data Subject Access should be made through the Facilities and Operational Management Team.

_Public information_
Copies of this Code of Practice are available to the public from the school website or Reception.