# IT SECURITY

| | |
|---|---|
| **Policy & Procedure No.** | **IT01** |
| **Reviewed & Updated:** | **November 2019** |
| **Next Review:** | **November 2020** |

# CONTENTS

## Reference to

LE01 Data Protection
LE02 Confidentiality
HR01 Anti Bullying and Harassment
HR02 Use of Social Media by Colleagues
The Education and Inspections Act 2006
The 2011 Education Act
ECS01 Positive Behaviour Support

## 1. Schedule for Development, Monitoring & Review

The implementation of this IT Security policy will be monitored by the Headteacher, The network manager/s and The School DPO

Monitoring will take place at regular intervals

The IT Security Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to IT Security or incidents that have taken place.

Should serious IT Security incidents take place; the following persons will be informed: Claire Collacott / Ben Kinslow or the School's DPO (Cantium Business Solutions). The Headteacher will be made aware as well.

The school will monitor the impact of the policy using

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity

## 2. Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other IT Security incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of, electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour or Mobile Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate IT Security behaviour that take place out of school.

## 3. Roles & Responsibilities

The following section outlines the IT Security roles and responsibilities of individuals and groups within the school:

### 3.1 The Governing Body

The Governing Body is responsible for the approval of the IT Security Policy and for reviewing the effectiveness of the policy. This will be carried out by them receiving regular information about IT Security incidents and monitoring reports. A member of the Board has taken on the role of IT Security Governor.

The role of the IT Security Governor will include:

- regular meetings with the Head teacher, in their role as IT Security Officer
- regular monitoring of IT Security incident logs from the technical staff
- regular monitoring of filtering / change control logs
- reporting to relevant Directors as required

### 3.2 The Headteacher

- has a duty of care for ensuring the safety (including IT Security) of members of the school community through their role as IT Security Officer.
- and Governing Body should be jointly aware of the procedures to be followed in the event of a serious IT Security allegation being made against a member of staff (the Headteacher is responsible for ensuring that relevant staff receive suitable training to enable them to carry out their IT Security roles and to train other colleagues, as relevant).
- will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal IT Security monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- should lead/chair the IT Security group.
- takes day to day responsibility for IT Security issues and has a leading role in establishing and reviewing the school IT Security policies / documents.
- ensures that all staff are aware of the procedures that need to be followed in the event of an IT Security incident taking place.
- provides training and advice for staff.
- liaises with the Governing Body, as necessary.
- liaises with school technical staff.
- receives reports of IT Security incidents and creates a log of incidents to inform future IT Security developments
- meets regularly with the relevant Governor to discuss current issues, review incident logs and filtering / change control logs.
- attends relevant meetings with the Governing Body.

### 3.4 Network Manager / Technical staff

The Network Manager / Technical Staff for ICT / Computing at Seadown is the responsibility of Ben Kinslow and Tula Rajwani for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required IT Security technical requirements and any Local Authority / other relevant body IT Security Policy / Guidance that may apply.
- that users may only access the networks and devices through properly enforced password protection settings, in which passwords are regularly changed.
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- that they keep up to date with IT Security technical information in order to effectively carry out their IT Security role and to inform and update others as relevant.
- that the use of the network / internet / Virtual Learning Environment / email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher.
- that monitoring software and systems are implemented and updated as agreed in school policies.

### 3.5 Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of IT Security matters and of the current school IT Security policy and practices.
- they have read, understood and signed the IT Security Policy.
- they report any suspected misuse or problem to the Head teacher for investigation / action / sanction.
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems.
- IT Security issues are embedded in all aspects of the curriculum and other activities.
- pupils understand and follow the IT Security Policy, with support as required.
- pupils have a good understanding, with support as required, of research skills and the need to avoid plagiarism and uphold copyright regulations (where appropriate).
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities and implement current policies with regard to these devices.
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

### 3.6 Child Protection / Safeguarding Designated Officer

This is currently the Deputy Headteacher; Claire Collacott. She is additionally trained in IT Security issues and is aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

### 3.7 Pupils

- are responsible for using the school digital technology systems in accordance with this policy (y*ounger pupils will be supported to understand what this means).*
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand, with support as required, school policies on the use of mobile devices and digital cameras. They will also taught to understand policies on the taking / use of images and on cyber-bullying.
- will be supported to understand the importance of adopting good IT Security practice when using digital technologies out of school and realise that the school's IT Security Policy covers their actions out of school, if their actions are related to their membership of the school.

### 3.8 Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, communication tools, website and information about national / local IT Security campaigns and literature. Parents and carers will be encouraged to support the school in promoting good IT Security practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website, communication tools and pupil records
- their children's personal devices in the school (where this is allowed)

### 3.9 Community Users

Community Users who access school systems / the school website etc. as part of the wider school provision will be expected to sign a Community User Agreement before being provided with access to school systems.

## 4. Policy Statements

### 4.1 Education –pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in IT Security is therefore an essential part of the school's IT Security provision. Children and young people need the help and support of the school to recognise and avoid IT Security risks and build their resilience.

**IT Security is a focus in all areas of the curriculum and staff will reinforce IT Security messages across the curriculum. The IT Security curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:**

- A planned IT Security curriculum will be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key IT Security messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- where appropriate, pupils should be helped to understand the need for the acceptable use of the IT systems and be encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit**.** The school will frequently monitor pupil use and appropriate software will be deployed to filter unsafe sites, as far as is possible.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

### 4.2 Education – parents / carers

Some parents and carers may have a limited understanding of IT Security risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of their children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site and online communication tools
- Parents / Carers evenings / sessions
- Reference to the relevant web sites / publications.

### 4.3 Education – The Wider Community

The school can provide opportunities for local community groups / members of the community to gain from the school's IT Security knowledge and experience. This may be offered through the following:

- IT Security messages targeted towards grandparents and other relatives, as well as parents.
- The school website will provide the IT Security Policy information for the wider community
- Supporting community groups e.g. Residential Settings, youth / sports / voluntary groups to enhance their IT Security provision *(for example by supporting the group in the use of Online Compass, an online safety self-review tool - www.onlinecompass.org.uk)*

### 4.4 Education & Training – Staff / Volunteers

It is essential that all staff receive IT Security training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All staff should receive IT Security training as part of their induction programme, ensuring that they fully understand the school IT Security policy.
- This IT Security policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The IT Security Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

### 4.5 Training – Governing Body

The Governing Body should take part in IT Security training / awareness sessions, with importance for those who are members of any sub-committee / group involved in technology and IT Security. This may be offered through:

- Participation in school training / information sessions for staff
- Factsheets and relevant links

## 5. Technical – Infrastructure, Equipment, Filtering & Monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their IT Security responsibilities:

***These people and the following systems in operation, are individually monitored by the DPO***

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by Ben Kinslow who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password if a breach is suspected.
- The passwords for the school ICT system, *looked after by JSPC: technical services* must also be available to the Headteacher and the other nominated person, Ben Kinslow, and kept in a secure place (e.g. secure folder).
- Ben Kinslow is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs).

- Internet access is filtered for all users. Illegal content is filtered using Metasearch software. Securus software is installed on the computers; this will flag up any reference to crime, sexually explicit images, bullying or any other inappropriate sites or language.
- Internet use is logged and regularly monitored.
- The school will endeavour to provide enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils etc.).
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the ICT Security Policy.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person (as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreement is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreement is in place regarding the extent of personal use that users (pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed system is in place that prevents staff from downloading executable files and installing programmes on school devices without proper permissions
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

## 6. Bring your own Device (BYOD) Policy

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of IT Security considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, GDPR, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy is be in place through the 'Community User Agreement'and reference made within all relevant policies.

- The school has a set of clear expectations and responsibilities for all users (Mobile Device Policy).
- The school adheres to the GDPR principles.
- All users are provided with and accept the IT Security Policy.
- All network systems are secure and access for different types of users is differentiated.
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises.
- All users will use their username and password and keep this safe.
- Mandatory training is undertaken for all staff.
- Pupils receive training and guidance on the use of personal devices.
- Regular audits and monitoring of usage will take place to ensure compliance.
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy.
- Any user leaving the school will follow the process outlined within the BYOD policy.

## 7. Use of Digital & Video Games

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 (mobile Device Policy) 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 on the internet e.g. on social networking sites.
- 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 GPDR). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- 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.
- Pupils 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.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers is obtained before photographs of pupils are published on the school website

## 8. GDPR

Personal data will be recorded, processed, transferred and made available according to the GPDR which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

**The school must ensure that:**

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a GDPR.
- It is registered as a Data Controller for the purposes of the GPDR.

- Responsible persons are appointed / identified - Data Protection Officer (DPO).
- Risk assessments are carried out.
- It has clear and understood arrangements for the security, storage and transfer of personal data.
- Data subjects have rights of access and there are clear procedures for this to be obtained.
- There are clear and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents.
- There are clear GDPR clauses in all contracts where personal data may be passed to third parties.
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

**Staff must ensure that they:**

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using secure, password protected, devices.

**When personal data is stored on any portable computer system, memory stick or any other removable media:**

- the data must be password protected.
- the device must offer approved virus and malware checking software.
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

## 9. Communications

*This is an area of rapidly developing technologies and uses. As things grow and develop, we will discuss amend and agree how we intend to implement and use these technologies (e.g. few schools allow pupils to use mobile phones in lessons, while others recognise their educational potential and allow their use. This may also be influenced and differentiated according to the age of the pupils).*

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

| | Staff | | | | Pupils | | | |
|---|---|---|---|---|---|---|---|---|
| **Communication Technologies** | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission | Not allowed |
| Mobile phones may be brought to school | | *x* | | | | | x | |
| Use of mobile phones in lessons | | *x* | | | | | | x |
| Use of mobile phones in social time | *x* | | | | | | | x |
| Taking photos on mobile phones / cameras | | | x | | | | | x |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Use of other mobile devices e.g. tablets, gaming devices | | x | | | | | x | |
| Use of personal email addresses in school, or on school network | | x | | | | | | x |
| Use of school email for personal emails | | | x | | | | x | |
| Use of messaging apps | | x | | | | | x | |
| Use of social media | | | x | | | | x | |
| Use of blogs | | x | | | | | x | |

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, messaging etc.), must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may be used at KS2 and above will be provided with individual school email addresses for educational use.
- Pupils will be taught about IT Security issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

## 10. Social Media – Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimize risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include acceptable use; social media risks; checking of settings; GDPR; reporting issues. Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

School staff should ensure that:

- No direct reference should be made in social media to pupils, parents / carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school.

- Security settings on personal social media profiles are regularly checked to minimize risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the IT Security group to ensure compliance with the ICT and Social Media/Mobile Device Policies.

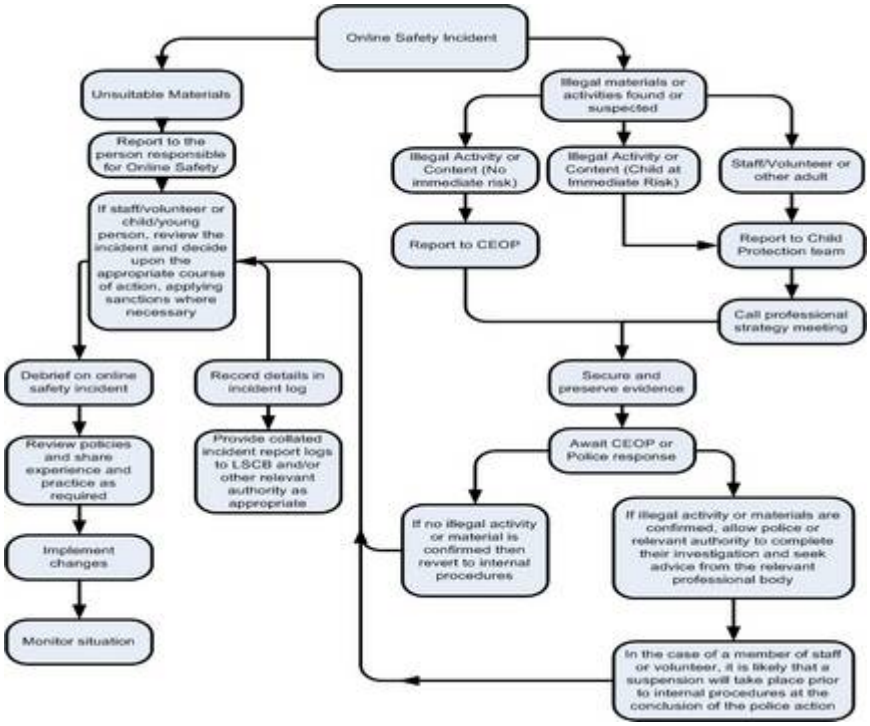
## 11. Unsuitable/Inappropriate Activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

## 12. Responding to Incidents of Misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the Flowchart for responding to online safety incidents and report immediately to the police and / or the DPO.




## 13. Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. All concerns must report to the network manager and / or the DPO.

## 14. School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

**END**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **POSITION** | Headteacher | **NAME** | | **SIGNATURE** | | **DATE** | |
| **POSITION** | Governor | **NAME** | | **SIGNATURE** | | **DATE** | |
| **POSITION** | | **NAME** | | **SIGNATURE** | | **DATE** | |