THOMAS JOHNSON LOWER SCHOOL
Hurst Grove, Lidlington, Bedfordshire MK43 0SB
Tel: 01525 402377 / 01525 404743
email: thomasjohnson@cbc.beds.sch.uk

e-Safeguarding Policy

Responsibility	All staff and the Governing Body
Review Date	September 2020
Approved by Full Governing Body	March 2018
Storage: (i) Electronic (ii) Hard Copy	(i) School website (managed by school secretary) (ii) School office and staff room

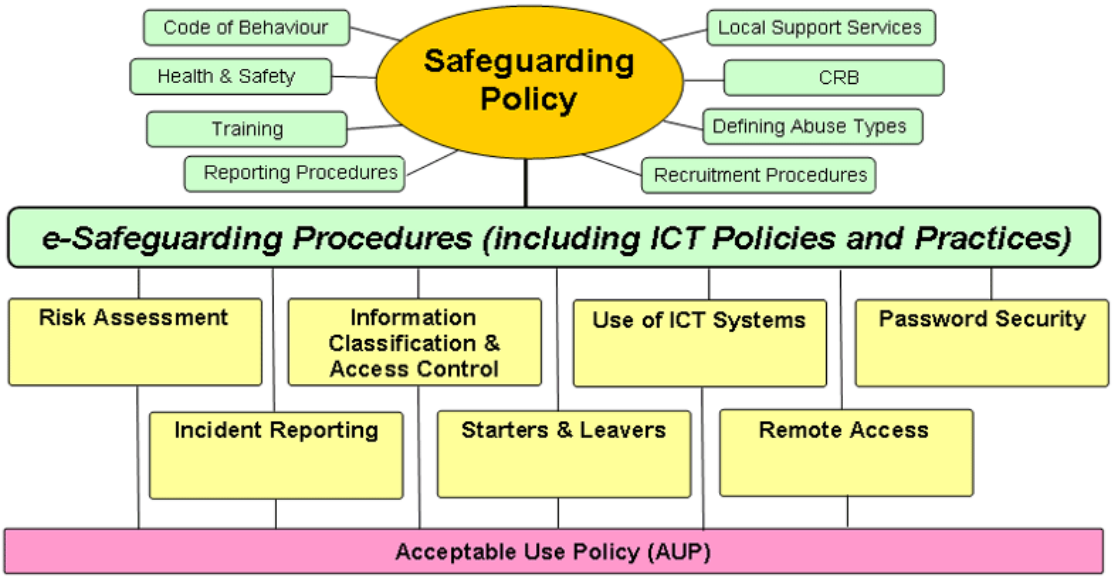
Rationale

Rapidly developing information and communication technologies (ICT) are exciting and motivating learning tools through which teaching and learning can be greatly enhanced. At Thomas Johnson Lower School we are committed to ensuring that ICT is used safely and responsibly and that risks related to ICT use are properly managed. The procedures outlined interpret the Becta guidelines and support the OFSTED safeguarding criteria.

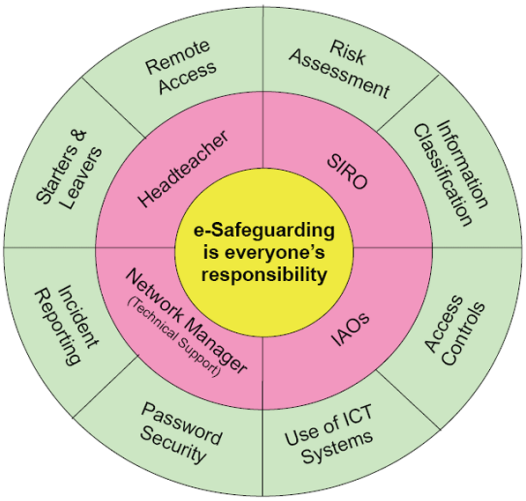
Framework

E-Safeguarding Procedures address all safeguarding issues which relate to the use of ICT. There are two main elements to these issues:

1. e-Security: procedures to ensure all electronic data is categorised as public, restricted or protected (see Information Classification below) and that electronic systems containing the data are securely maintained (see Risk Assessment below)
2. e-Safety: procedures to ensure all members of the school community know their access rights and responsibilities in using ICT. These procedures are expressed in the school's Acceptable Use Policy (AUP).



Roles and Responsibilities



1. *Senior Information Risk Owner (SIRO)*

Overall responsibility for e-Safeguarding rests with the Head Teacher who is also the designated SIRO:

a) owns the information risk policy and risk assessment;

b) keeps a record of all Information Asset Owners (IAOs) – see below;

c) is accountable to governors for matters relating to e-safeguarding.

2. *Information Asset Owners (IAOs)*

These include any members of staff who compile specific information about children or staff and their role is to be clear about:

a) what information they hold, and for what purposes;

b) how this information will be amended or added to over time;

c) who has access to the data and why;

d) how information is retained and disposed of in line with GDPR procedures.

They include all teachers and teaching assistants and the school secretary.

3. *Network Manager* *(or whoever oversees the network, monitoring its performance, security, error detection, and implements access controls)* ***and ICT Lead.***

The role of Network Manager is currently performed almost exclusively by our ICT technician from Partnership Education who works under the supervision of the head teacher and other members of staff. The school has its own ICT Lead, who is the key contact with the ICT technician with regard to software upgrades, faults, and who performs a weekly system back-up.

Other network tasks are sometimes carried out by the head teacher, technical staff from Central Bedfordshire or external organisations (e.g. Espresso, Netmedia).

Remote monitoring of the network and systems is carried out by a contractor who follows our safeguarding procedure.

NB

Although these roles are specifically referred to in the procedures below, maintaining data security is everyone's responsibility - whether they are a member of staff, a student, a parent or a governor. It is recognised that failure to apply agreed controls to secure data can be a serious matter, even resulting in legal action.

E-Safeguarding Procedures

1. Risk Assessment (Responsibility: Head teacher/SIRO; ICT Lead; Key Stage Leaders)

E-Security and e-Safety is based upon the assessment of risk, and the implementation of controls to manage these risks; no use of ICT is completely risk free. Information security is critical, in both protecting the information held concerning staff and pupils, and in ensuring the reliability of ICT systems to support teaching and learning.

The risk assessment is updated and reviewed annually by the above staff and reported to the Governing Body.

[See the Risk Assessment Form below]

2. Information Classification (Responsibility: All Staff)

These classification levels are derived from the potential impact that unauthorised disclosure of information may have on the individuals concerned.

i. **Restricted:** information which can only be accessed by named individuals or groups. **Printed restricted information will be labelled to identify it as confidential.** Where possible, restricted information on screen should be labelled as such.

ii. **Protected:** general school information which is not expected to be released to the public.

iii. **Public:** Information freely available to anyone.

3. Access Control: Systems Access (Responsibility: Head teacher/SIRO; ICT Lead; Key Stage Leaders)

a) Access to all ICT systems is via unique login and password.

b) Where possible, all information storage is restricted to just necessary users. Access granted to new groups of users (for example, an external group attending a school-based event) is under the approval of the SIRO.

c) All requests for access beyond that normally allocated (e.g. teachers wishing to access pupil personal storage) will be authorised by the SIRO. This includes the authorisation of access required by the ICT Support Team during investigations.

d) Where 'restricted' information is stored, access will only be granted to individuals approved by the SIRO.

e) Access controls are reviewed to ensure that any users who leave have their access removed.

4. Access Control: The Network (Responsibility: ICT Technician)

a) Where any external network traffic is allowed from the Internet to the school, a local firewall is to be deployed to restrict traffic to only necessary ports and IP addresses.

b) All Internet-facing systems are placed onto a separate network segment; a de-militarised zone (DMZ), with access controlled by a firewall.

c) Where externally facing services may be at particular risk, the addition of an Intrusion Prevention System (IPS) is used.

d) The use of external specialist third-party testing may be considered on an annual basis for Internet visible systems.

5. Use of ICT Systems (Responsibility: All Staff)

a) All users of ICT systems are responsible for their own use of technologies, taking appropriate steps to ensure that they use technology safely, responsibly and legally, so that the school is not exposed to risks including virus attacks, compromise of network systems and services, legal issues, and ensuring pupil safety.

b) Staff and pupils are aware that all school ICT activity and on-line communications may be monitored, including any personal and private communications made via the school network.

c) All staff are made aware of the school's Social Networking Policy, and sign to show they have read, understood and accept the policy contents.

d) Appropriate additional training is made available to members of the school community. This will cover:

   i. School Workforce training for all e-safeguarding procedures and the consequences of inappropriate practice;

   ii. School Workforce training in responsible approaches to data on mobile devices, communicating online and procedures when using multimedia digital content such as photographs, videos and podcasts in terms of permission seeking, taking, storage and retention according to the school's GDPR compliance guidance;

   iii. An e-safety curriculum for pupils referenced in schemes of work and programmes of study. The programme could include the responsible use of web and communication technologies both inside and outside school and risks related to cyber-bullying;

   iv. Regular review of the AUP with children, staff and governors;

   v. ICT non-teaching staff training related to how ICT can enhance teaching and learning.

   vi. Material from organisations like ChildNet, ThinkUKnow, CEOP and It's Learning (Netmedia) may be useful in addressing training needs.

e) The school has a working Acceptable Use Policy (AUP) based on all the agreed procedures for e-security and e-safety and covering ICT usage by all sectors of the school community. This policy will be subject to annual review by the governing body.

f) Parents are made aware of the requirements of the AUP (e.g. through newsletters, through the school prospectus).

6. Password Security (Responsibility: All Staff)

Passwords are an important aspect of information security and are the usual way to protect access to information. All members of staff with access to ICT systems are responsible for taking the appropriate steps to select and maintain secure passwords.

These steps include:

a) Keeping their password secure from pupils, family members, and other staff.

b) Using a different password for accessing school systems to that used for personal (non-school) purposes.

c) Choosing a password that is difficult to guess, or difficult for pupils to obtain by watching staff login.

d) Adding numbers or special characters (e.g. !@£$%^) to their passwords.

e) Changing passwords regularly e.g. each school term.

f) Staff should try not to write down their password, unless absolutely necessary and then in a location that cannot be accessed by anyone else. In addition, when leaving a computer for any length of time, staff **shall** ensure a screen saver + password unlock appears so that documents are not left visible. Alternatively, staff should log off or lock the computer, using CTRL+ATL+DELETE.

7. Incident Reporting (Responsibility: head teacher)

An important element of e-safeguarding is the ability to identify and deal with incidents related to the confidentiality of information. All staff and pupils have a responsibility to report e-safety or e-security incidents so that they may be dealt with effectively and in a timely manner in order to minimise any impact on the school.

Incidents are reported to the Head teacher who records/logs them on CPOMS (our on-line safeguarding tool). When necessary, the risk assessment will be updated in light of new incidents. The Log and any action plans will be brought to the attention of the Governing Body at the next Full Governing Body meeting.

Incidents for the log might include:

- Circumventing the network security system;
- Accessing inappropriate material;
- Installing unapproved software;
- Using other people's email addresses or passwords;
- Breaching copyright;
- Uploading school material onto a social network or chat room;
- Leaving school mobile devices (e.g. laptops) unattended or unsecured.

8. Starters and Leavers (Responsibility: School secretary; network manager)

a) The head teacher ensures that the above staff are informed promptly of any member of staff joining or leaving the school.

b) Any school owned computer equipment is returned on exit.

c) The above staff will ensure that leavers' access is removed, or disabled, in a timely manner.

d) There will be a similar process for pupils starting or leaving the school.

9. Remote Access (Responsibility: All Staff)

Users of mobile computing facilities (such as laptops; smartphones/tablets) are responsible for safeguarding such equipment and should take all responsible precautions to prevent theft, loss or damage of such items, and to prevent unauthorised access to information held on the device. Staff are reminded to take particular care should when leaving devices in cars, hotel rooms, or the home, ensuring that they are not visible. Where possible, mobile devices should be locked away when not in use.

The following guidelines will apply when accessing systems and information away from the school:

a) Only necessary information will be stored on the device;

b) Pupil sensitive (restricted) information will not be stored on any mobile devices unless encrypted or protected by a secure password.

The removal of any ICT equipment, information and software from school premises will only be permitted with prior authorisation from the ICT Co-ordinator/SIRO/Head Teacher.

Remote access to network/stored data:

a) No remote access to the school network will be allowed except by contracted technical support staff who are required to monitor the network and Internet;

b) Remote access to web-based data will be through the password provisions;

c) Passwords for remote access to web-based data and data systems will be known only to the school secretary and the head teacher**.**

10. Technical Security (Responsibility: ICT Technician; ICT Lead; head teacher)

a) All externally facing devices are hardened and patched to ensure no high-risk vulnerabilities are present, with security updates applied promptly. All other internal systems will be regularly patched with the latest security updates, ideally at the beginning of each term.

b) The use of a scanner, to help identify high-risk vulnerabilities, will be considered.

c) All desktops will have up-to-date anti-virus software installed.

d) All incoming email will be scanned for viruses and filtered for spam.

e) All virus definitions will be updated regularly.

f) All anti-virus will be configured to alert the ICT technician when any virus is detected.

g) Where possible, the use of memory sticks and other mobile storage media will be scanned for viruses each time they are connected.

h) All pupil access to the Internet will be filtered for inappropriate content.

i) Children will not be allowed to use search engines to find information except when searching within closed systems (e.g. Espresso, Britannica on line).

j) All hard disks and other media containing school information will be securely deleted, either by specialist deletion utilities or physical destruction, prior to disposal.

k) Backup media will be subject to the same security controls and destruction procedures as other ICT storage devices.

This policy links to:

- Safeguarding policy
- Social Networking policy

e-Safeguarding Risk Assessment Form

High Impact: Public exposure of restricted information leading to embarrassment, system downtime, or data corruption impacting learning & teaching.

Medium Impact: Exposure of protected information to a non-authorised third party, leading to outcomes listed above.

Low Impact: Internal exposure of information beyond authorised individuals leading to outcomes listed above.

E-Security and/or e-safety issue (risk assess these plus others identified)	**Threat** (What could happen)	**Impact** [See definitions above] High: Score 3 Medium: Score 2 Low: Score 1		**Vulnerability** (What is it you do – or not do – that could lead to the threat materialising)	**Likelihood** High(3): next 6 month Medium(2): next 2 yrs Low(1): unlikely in next 2 years		**Total Score** (Impact x Likelihood; out of 9)	**Action Plan** (Either risk accepted OR actions to be taken to reduce risk)
Information (restricted/protected) taken out of school on laptop, email etc	**Unsanctioned use of information through loss or theft**		**3**	**Vulnerability only should storage of laptops be unsafe etc or non-use of encryption/secure password**	**No previous occurrences**	**1**	**3**	**Risk accepted. Staff clearly briefed on risk assessment. Encryption/secure passwords are used.**
Use of mobile data storage e.g. memory sticks	**Unsanctioned use of information through loss or theft**		**3**	**Vulnerability only should storage of memory sticks etc be unsafe or non-use of encryption/secure password**	**No previous occurrences**	**1**	**3**	**Risk accepted provided. Staff clearly briefed on risk assessment. Encryption/secure passwords are used**
Use of Internet for data transfer and communication	**Children exposed to inappropriate content**		**3**	○ **All Internet access through schools website so that filtering is available** ○ **No use of Internet search engines by children**	**No previous occurrence**	**1**	**3**	**Risk accepted with current safeguards in place.**
Pupil gaining access to restricted or protected information	**Staff data seen by children**		**2**	**Staff data only to be available via secure password**	**No previous occurrence**	**1**	**2**	**Risk accepted with current safeguards**
Back up (storage)	**Data lost because of theft or damage (or see mobile data above)**		**3**	**Back up carried out regularly and stored securely**	**No previous occurrence – web based data means less reliance on mobile storage**	**1**	**3**	**Risk accepted with current safeguards**

E-Security and/or e-safety issue (risk assess these plus others identified	**Threat** (What could happen)	**Impact** [See definitions above] High: Score 3 Medium: Score 2 Low: Score 1		**Vulnerability** (What is it you do – or not do – that could lead to the threat materialising)	**Likelihood** High(3): next 6 month Medium(2): next 2 yrs Low(1): unlikely in next 2 years		**Total Score** (Impact x Likelihood; out of 9)	**Action Plan** (Either risk accepted OR actions to be taken to reduce risk)
Password misuse or poorly managed	**Staff data seen by children or other staff**		**1**	**Staff sharing passwords or using predictable passwords**	**No previous complaints/occurrences**	**2**	**2**	**Risk accepted with the proviso that agreed rules are followed:** **Secure passwords** **Termly change of password** **Previous passwords not accepted** **No sharing of passwords** **Leavers' access promptly removed**
Virus and malicious software installs	**Data/systems corrupted – loss of curriculum or admin capability**		**2**	**Virus/malicious software introduced via email/mobile storage devices**	**No previous occurrence**	**2**	**4**	**Risk accepted with current safeguards:** **Anti-virus precautions** **Regular virus updates** **LA filtering**
Inadequate pupil training in e-security and e-safety	**Children not aware of simple rules for their safety – unprepared for possible danger – possibly at risk when using Internet technologies out of school**		**3**	**Scheme of work for e-safety ensures children fully aware of simple rules for their safety.**	**No known occurrence of children putting themselves at risk**	**1**	**3**	**Risk accepted with current safeguards:** **Children taught e-safety rules** **e-safety rules highly visible in ICT suite** **assemblies promote children's safety.**

E-Safeguarding Procedures: March 2018

Procedure	In Place	Partially in place	Not in place	Don't know	Actions for consideration
Roles and Responsibilities: SIRO appointed, IAOs identified and listed, technician responsibilities specified, Data Protection Officer appointed	✓				
1. Risk Assessment: Procedures established, assessments and remedial action plans documented	✓				
2. Information Classification: Table created and system for classification labelling established	✓				
3. Access Controls: *Systems access records* (who has access to what) and *Network security measures* established and implemented	✓				
4. Use of ICT Systems: AUP 'owned' by everyone. On-going education & training programme for everyone	✓				
5. Password Security: Minimum requirements in place	✓				
6. Incident Reporting: Procedure in use and monitored with action taken as necessary	✓				
7. Starters and Leavers: Procedures established and active for both staff and pupil records	✓				
8. Remote Access: Minimum requirements in place	✓				
9. Technical Security: Minimum requirements in place	✓				
10. Other: GDPR compliance		√			Encrypted memory sticks for all staff members to be purchased. Data audit to identify location of all Protected Personal Information underway.