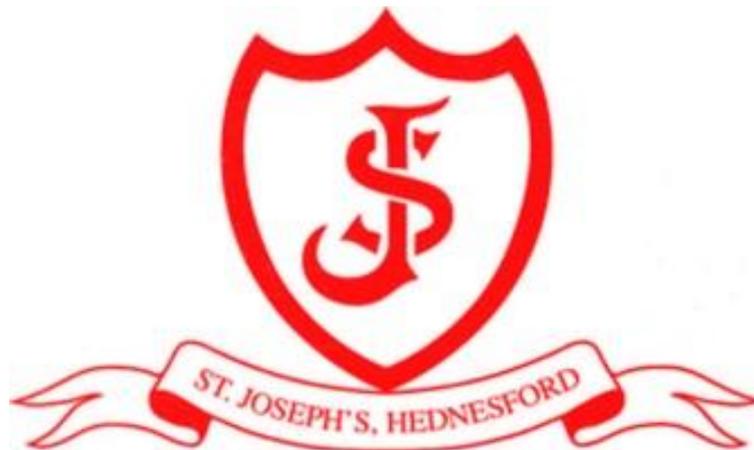


# St Joseph's Catholic Primary School and Nursery, Hednesford

- THIS DOCUMENT IS THE SCHOOL'S INFORMATION SECURITY POLICY.
- IT WAS APPROVED by the governing body on 11<sup>th</sup> July 2018
- THIS POLICY WILL BE REVIEWED bi-annually.
- NEXT REVIEW: July 2020



Signed:

---

CHAIR

DATE

## Introduction

ICT in the 21<sup>st</sup> Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- Email, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases).

At St Joseph's Catholic Primary School, we understand the responsibility to educate our pupils on eSafety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them, to ensure confidentiality and integrity.

The purpose of this policy is to ensure that data is held securely and that all staff and members of the school community understand and are compliant with the school's procedures.

Both this policy and the Acceptable Use Agreement (for all staff, governors, regular visitors [for regulated activities] and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

## Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact the Headteacher. Any ICT authorised staff member will be happy to comply with this request.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 2018, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the email of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

## **Asset Register**

School will hold an asset register including data assets and hardware assets. This is kept on the school admin computer and maintained by the Bursar

## Breaches

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

The severity of a policy breach may be grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated.

Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £20million for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations' processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

For pupils, reference will be made to the school's behaviour policy.

---

## Incident Reporting

### Definition

A personal data breach means "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provisions of a public electronic communications service."

A data security breach can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood

- Hacking attack
- ‘Blagging’ offences where information is obtained by deceiving the organisation who holds it

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported using GDPRiS. GDPRiS is an online system (<https://app.gdpr.school>) Additionally, all security breaches, lost/stolen equipment or data (including remote access and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported using GDPRiS. All breaches will be investigated. The following will occur should a breach take place.

## **Action**

However the breach has occurred, there are four important elements to any breach management plan:

### 1. Containment and recovery

Data security breaches will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. This will often involve input from specialists such as IT, HR and legal and in some cases contact with external stakeholders.

Should a data breach occur at St Joseph’s, the school DP staff member will:

- Take the lead on investigating the breach, ensuring that appropriate resources are available.
- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This could be isolating or closing a compromised section of the network, finding a lost piece of equipment or simply changing the access codes at the front door.
- Establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause. As well as the physical recovery of equipment, this could involve the use of back up tapes to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.
- Where appropriate, inform the police.
- Dependent upon the severity of the breach the Head Teacher and Data Protection Officer may be informed.

### 2. Assessing the risks

Some data security breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. An example might be where a laptop is irreparably damaged but its files were backed up and can be recovered. Before deciding on what steps are necessary, we will assess the risks which may be associated with the breach. We will carry out an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen. To do this, we will consider the following points:

- What type of data is involved?

- How sensitive is it?
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data? If data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relate?
- Regardless of what has happened to the data, what could the data tell a third party about the individual?
- How many individuals' personal data are affected by the breach?
- Who are the individuals whose data has been breached?
- What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service you provide?

### 3. Notification of breaches

Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.

When deciding whether a breach requires informing people or organisations, the following will be considered:

- Are there any legal or contractual requirements?
- Can notification help meet the schools security obligations whereby appropriate technical and organisational measures should be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data?
- Can notification help the individual? Bearing in mind the potential effects of the breach, could individuals act on the information you provide to mitigate risks, for example by cancelling a credit card or changing a password?
- If a large number of people are affected, or there are very serious consequences, you should inform the ICO.
- How can notification be made appropriate for particular groups of individuals, for example, if you are notifying children or vulnerable adults.

The school DP staff member will consider who to notify, what they will be told and how the message will be communicated. This will depend to a large extent on the nature of the breach but the following points will be considered when making decisions:

- If a data breach occurs, the school may inform the Chair or Governors
- Contact may be made with the Information Governance Unit at Staffordshire County Council. Depending on the level of the breach, they may then require the school to notify the ICO.
- Any notification will at the very least include a description of how and when the breach occurred and what data was involved. Data breaches will be recorded on the GDPRiS system. Details of what the school has already done to respond to the risks posed by the breach should also be included.
- When notifying individual's specific and clear advice will be given on the steps they can take to protect themselves and also what the school can do to help them.

Should the data breach be reported to the ICO, details of the security measures in place such as encryption and, where appropriate, details of the security procedures the school had in place at the time the breach occurred will be included. If the media become aware of the breach, the ICO will also be notified so that they can support the school in managing enquiries.

#### 4. Evaluation and response

It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of the school's response to it. Following any breach, the school will identify where improvements to data protection procedures can be made. The school will:

- Review what personal data is held and where and how it is stored.
- Establish where the biggest risks lie and ensure that appropriate measures are in place to minimise the risk of further security breaches.
- Ensure that not only is the method of transmission secure but also that the school only shares or discloses the minimum amount of data necessary. By doing this, even if a breach occurs, the risks are reduced
- Identify weak points in the existing security measures such as the use of portable storage devices or access to public networks
- Monitor staff awareness of security issues and look to fill any gaps through training or tailored advice.

Any data security breaches will be recorded on the GDPRiS system. A review of any breaches will be shared termly with Governors at the Health & Safety Committee meeting.

## **Clear Desk Policy**

The school policy is that all confidential information will be locked away when a member of staff is not at their desk.

Computers/laptops should be screen locked when a member of staff leaves their workstation.

## Computer Viruses

- All files downloaded from the Internet, received via email or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.
- Never interfere with any anti-virus software installed on school ICT equipment.
- If your machine, including teacher laptop is not routinely connected to the school network, you must make provision for regular virus updates through your IT team.
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

## Data Security

### Data Protection: key responsibilities for School Heads and Governors

The accessing and appropriate use of school data is taken very seriously.

---

#### Security

- The school gives relevant staff access to its Management Information System, with a unique username and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times
- It is the responsibility of individual staff to ensure the security of any personal or sensitive information contained in documents faxed, copied, scanned or printed. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used

---

#### Relevant Responsible Persons

Senior members of staff should be familiar with information risks and the school's response. The Headteacher has the following responsibilities:

- they lead on the information risk policy and risk assessment
- they advise school staff on appropriate use of school technology
- they act as an advocate for information risk management

The Office of Public Sector Information has produced [Managing Information Risk](http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf), [\[http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf\]](http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf) to support relevant responsible staff members in their role.

## Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data
- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen
- Disposal of any ICT equipment will conform to:

The Waste Electrical and Electronic Equipment Regulations 2006

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

<http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx>

[http://www.opsi.gov.uk/si/si2006/uksi\\_20063289\\_en.pdf](http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf)

[http://www.opsi.gov.uk/si/si2007/pdf/uksi\\_20073454\\_en.pdf?lang=e](http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=e)

Data Protection Act 2018

<https://ico.org.uk/for-organisations/education/>

Electricity at Work Regulations 1989

[http://www.opsi.gov.uk/si/si1989/Uksi\\_19890635\\_en\\_1.htm](http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm)

- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal
- The school's disposal record will include:
  - Date item disposed of
  - Authorisation for disposal, including:
    - verification of software licensing
    - any personal data likely to be held on the storage media? \*
  - How it was disposed of e.g. waste, gift, sale
  - Name of person & / or organisation who received the disposed item

\* if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.

- Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate

Further information available at:

## **Waste Electrical and Electronic Equipment (WEEE) Regulations**

### **Environment Agency web site**

Introduction

<http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx>

The Waste Electrical and Electronic Equipment Regulations 2006

[http://www.opsi.gov.uk/si/si2006/uksi\\_20063289\\_en.pdf](http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf)

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

[http://www.opsi.gov.uk/si/si2007/pdf/uksi\\_20073454\\_en.pdf?lang=e](http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=e)

### **Information Commissioner website**

<https://ico.org.uk/>

**Data Protection Act – data protection guide, including the 6 principles**

<https://ico.org.uk/for-organisations/education/>

### **PC Disposal – SITSS Information**

[http://www.thegrid.org.uk/info/traded/sitss/services/computer\\_management/pc\\_disposal](http://www.thegrid.org.uk/info/traded/sitss/services/computer_management/pc_disposal)

## Email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and how to behave responsible online.

Staff and governors should use a school email account for all official communication to ensure that children are protected through the traceability of all emails through the school email system. In addition, it is important that governors are protected against possible allegations of inappropriate contact with children. This is to help mitigate the chance of issues occurring and is an essential element of the safeguarding agenda.

---

### Managing email

- The school gives all teaching staff and administration staff their own email account to use for all school business as a work based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed
- Staff should use their school email for all professional communication.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. The school email account should be the account that is used for all school business
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses
- All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Staff sending emails to external organisations, parents or pupils are advised to cc. the Headteacher, line manager or designated line manager
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- Emails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your email account as follows:
  - Delete all emails of short-term value
  - Organise email into folders and carry out frequent house-keeping on all folders and archives

- Staff must inform (the eSafety coordinator or line manager) if they receive an offensive email
- Pupils are introduced to email as part of the Computing Programme of Study
- However you access your school email (whether directly, through webmail when away from the office or on non-school hardware) all the school email policies apply

---

## **Sending emails**

- If sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section Emailing Personal or Confidential Information
- Use your own school email account so that you are clearly identified as the originator of a message
- Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- School email is not to be used for personal advertising

---

## **Receiving emails**

- Check your email regularly
- Activate your 'out-of-office' notification when away for extended periods
- Never open attachments from an untrusted source; consult your network manager first
- Do not use the email systems to store attachments. Detach and save business related work to the appropriate shared drive/folder
- The automatic forwarding and deletion of emails is not allowed

---

## **Emailing Personal or Confidential Information**

- Where your conclusion is that email must be used to transmit such data:

Obtain express consent from your manager to provide the information by email and exercise caution when sending the email and always follow these checks before releasing the email:

- Encrypt and password protect. See <http://www.thegrid.org.uk/info/dataprotection/#securedata>
  - Verify the details, including accurate email address, of any intended recipient of the information
  - Verify (by phoning) the details of a requestor before responding to email requests for information
  - Do not copy or forward the email to any more recipients than is absolutely necessary
- 
- Do not send the information to any person whose details you have been unable to separately verify (usually by phone)
  - Send the information as an encrypted document **attached** to an email
  - Provide the encryption key or password by a **separate** contact with the recipient(s)
  - Do not identify such information in the subject line of any email
  - Request confirmation of safe receipt

## Equal Opportunities

---

### **Pupils with Additional Needs**

The school endeavours to create a consistent message with parents/carers for all pupils and this in turn should aid establishment and future development of the schools' eSafety rules.

However, staff are aware that some pupils may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

## Acceptable Use Agreement: Pupils - Primary

### Primary Pupil Acceptable Use Agreement / eSafety Rules

#### Key Stage 1

- I will only use the internet when an adult is with me
- I will tell my teacher if I am scared
- I can click on the buttons or links when I know what they are
- I can search the internet with an adult
- I can write polite and friendly emails to people that I know
- I can send and open emails with an adult
- I always ask for help if I get lost on the internet

#### Key Stage 2

- I will only use ICT in school for school purposes
- I will only use my class email address or my own school email address when emailing
- I will only open email attachments from people I know, or who my teacher has approved
- I will not tell other people my ICT passwords
- I will only open/delete my own files
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- I will not look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately
- I will not give out my own/others details such as name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the

school community

- I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher
- I will not bring a Smart Watch to school because I am not allowed to wear one during the school day
- I will not sign up to online services until I am old enough

## School logo and details

Dear Parent/ Carer

ICT including the internet, email and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact school.

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.



### **Parent/ carer signature**

We have discussed this document with .....(child's name) and we agree to follow the eSafety rules and to support the safe use of ICT at St Joseph's Catholic Primary School.

Parent/ Carer Signature .....

Class ..... Date .....

# Acceptable Use Agreement: Staff, Governors and Visitors

## Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to pupils
- I will only use the approved, secure email system(s) for any school business
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick
- I will not install any hardware or software without permission of the Headteacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher
- I will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community'
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies
- I will not use personal electronic devices (including smart watches) in public areas of the school between the hours of 8.30am and 3.30pm, except in the staff room and where there are signs to indicate this.

### User Signature

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

Signature ..... Date .....

Full Name ..... (printed)

Job title .....

---

## Misuse and Infringements

### Complaints

Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator or Headteacher. Incidents should be logged and the **Flowcharts for Managing an eSafety Incident** should be followed.

### Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation by the Headteacher. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)
- Users are made aware of sanctions relating to the misuse or misconduct through this policy.

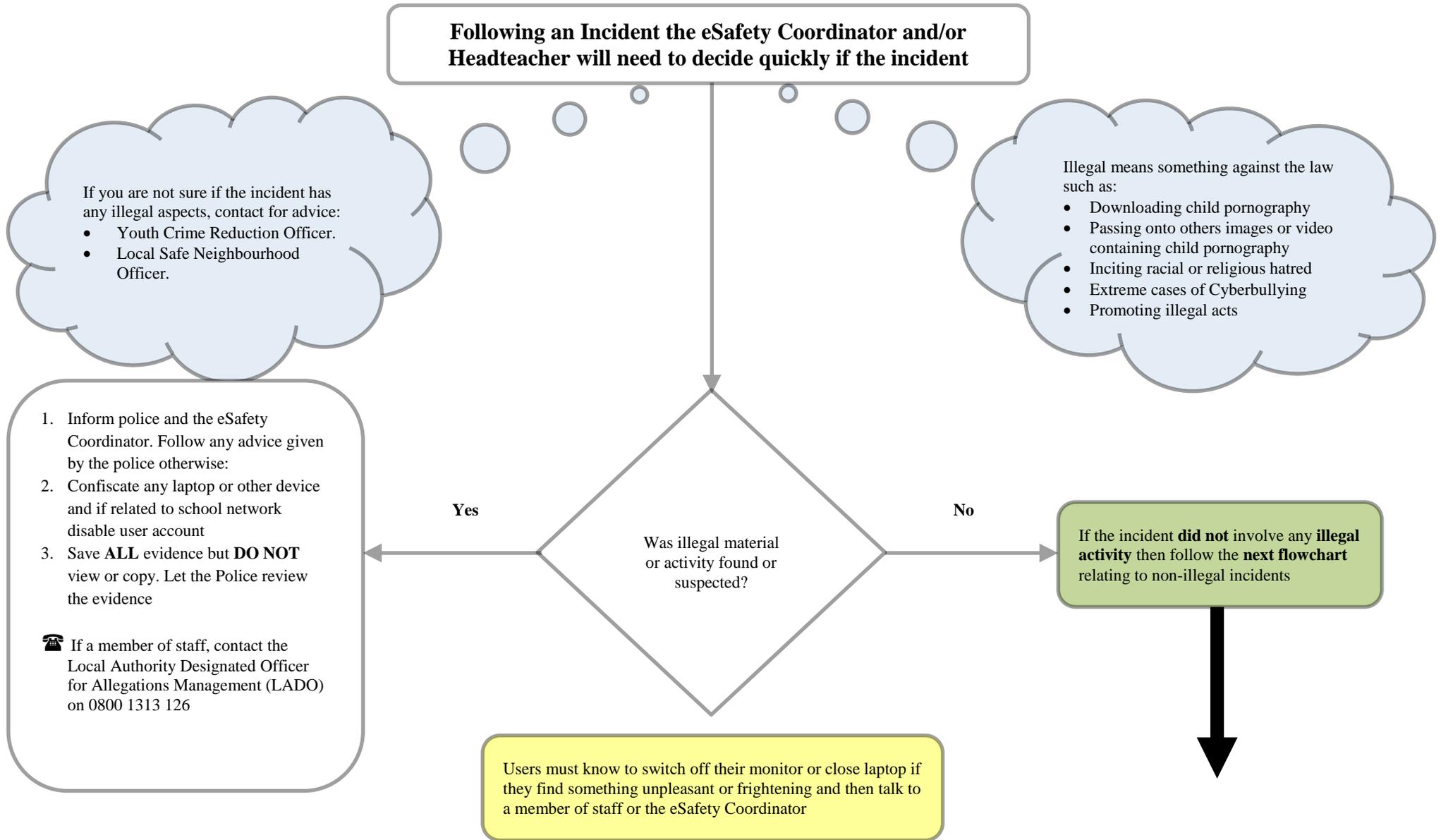
---

## Flowcharts for Managing an eSafety Incident

These three flowcharts have been developed by the HSCB eSafety subgroup and are designed to help schools successfully manage eSafety incidents

<http://www.thegrid.org.uk/eservices/safety/incident.shtml>

## Flowchart to support decisions related to an illegal eSafety Incident For Headteachers, Senior Leaders and eSafety Coordinators



If the incident **did not** involve and illegal activity then follow this flowchart

## Managing an eSafety Incident Flowchart For Headteachers, Senior Leaders and eSafety Coordinators

The eSafety Coordinator and/ or Headteacher should:

- Record in the school eSafety Incident Log
- Keep any evidence

If member of staff has:

- Behaved in a way that has harmed a child, or may have harmed a child.
- Possibly committed a criminal offence against or related to a child; or
- Behaved towards a child or children in a way that indicates he or she would pose a risk of harm if they work regularly or closely with children.

Contact the LADO on: 0800 1313 126, then follow the bullet points below:

- Review the evidence and determine if the incident is accidental or deliberate
- Decide upon the appropriate course of action
- Follow the school disciplinary procedures (if deliberate)

Incident could be:

- Using another person's user name and password
- Accessing websites which are against school policy e.g. games, social networks
- Using a mobile phone to take video during a lesson
- Using the technology to upset or bully

Yes

Did the incident involve a member of staff?

No

Pupil as victim

Was the child the victim or the instigator?

Pupil as instigator

In – school action to support pupil by one or more of the following:

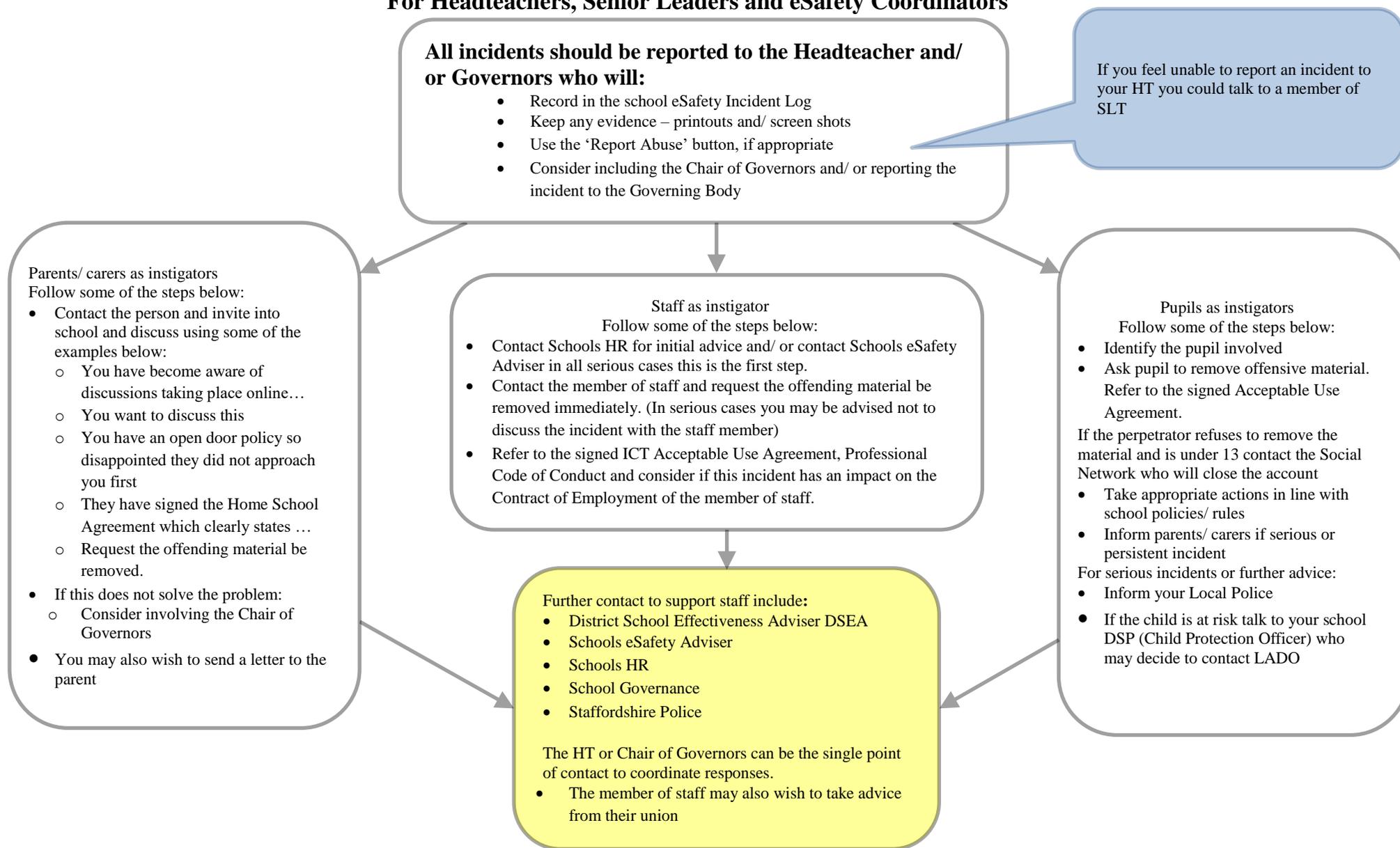
- Class teacher
- eSafety Coordinator
- Senior Leader or Headteacher
- Designated Senior Person for Child Protection (DSP)
- School PCSO

Inform parents/ carer as appropriate  
If the child is at risk inform CSPLO immediately  
Confiscate the device, if appropriate.

- Review incident and identify if other pupils were involved
- Decide appropriate sanctions and/ or support based on school rules/ guidelines
- Inform parents/ carers if serious or persistent incident
- In serious incidents consider informing the CPSLO as the child instigator could be at risk
- Review school procedures/ policies to develop best practice

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and then talk to a member of staff or the eSafety Coordinator

## Managing an eSafety Incident Flowchart involving staff as victims For Headteachers, Senior Leaders and eSafety Coordinators



## Internet Access

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All internet use through St Joseph's network is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

---

### Managing the Internet

- The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity
  - Staff will preview any recommended sites, online services, software and apps before use
  - Searching for images through open search engines is discouraged when working with pupils
  - If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
  - All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
  - All users must observe copyright of materials from electronic resources
- 

### Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience
- Do not reveal names of colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application
- On-line gambling or gaming is not allowed

It is at the Headteacher's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.

---

### Infrastructure

- St Joseph's Catholic Primary School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 2018, The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998

- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required
- The school does not allow pupils access to internet logs
- The school uses management control tools for controlling and monitoring workstations
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate
- It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines
- Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the network managers to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given to the **(technician/teacher)** for a safety check first
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Headteacher.
- If there are any issues related to viruses or anti-virus software, the network manager should be informed by detailing the issue in the book located on the iPad trolley.

## Managing Other Online Technologies

Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavors to deny access to social networking and online games websites to pupils within school
- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online
- Our pupils are asked to report any incidents of Cyberbullying to the school
- When signing up to online services that require the uploading of what could be deemed as personal or sensitive data, school would in the first instance carry out a protection impact assessment.
- Services such as Facebook and Instagram have a 13+ age rating which should not be ignored

## Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting eSafety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website)
- Parents/carers are expected to sign a Home School agreement containing the following statement(s)
  - **I/we will support the school approach to online safety and not upload or add any text, image, sound or videos that could upset or offend any member of the school community, or bring the school name into disrepute.**
  - **I/we will ensure that my/our online activity would not cause the school, staff, pupils or others distress or bring the school community into disrepute.**
  - **I/we will support the school's policy and help prevent my/our child/children from signing up to services such as Facebook, Instagram, Snapchat and YouTube whilst they are underage (13+ years in most cases).**
  - **I/we will close online accounts if I/we/teachers find that these accounts are active for our underage child/children.**
- The school disseminates information to parents relating to eSafety where appropriate in the form of;
  - Information evenings
  - Practical training sessions e.g. current eSafety issues
  - Posters
  - School website information
  - Newsletter items

## Passwords and Password Security

---

### Passwords

Please refer to the document on the grid for guidance on How to Encrypt Files which contains guidance on creating strong passwords and password security

<http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata>

- **Always use your own** personal passwords
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- **Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else.** Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- **Never tell a child or colleague your password**
- **If you aware of a breach of security with your password or account inform the Headteacher immediately**
- Passwords must contain a minimum of six characters and be difficult to guess
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols
- User ID and passwords for staff and pupils who have left the school are removed from the system within 1 month of leaving.
- **If you think your password may have been compromised or someone else has become aware of your password report this to your ICT support team.**

---

### Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords private and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety Policy and Data Security
- Users are provided with an individual network, email, and Management Information System log-in username.
- Pupils are not permitted to deliberately access on-line materials or files on the school network or local storage devices of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS systems and/or learning platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. The automatic log-off time for the school network is 3 minutes.

---

## **Zombie Accounts**

Zombie accounts refers to accounts belonging to all users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the school has left
- Prompt action on disabling accounts will prevent unauthorised access
- Regularly change generic passwords to avoid unauthorised access

## Personal or Sensitive Information

---

### Protecting Personal or Sensitive Information

- Ensure that any school information accessed from your own PC or removable media equipment is kept secure, and remove any portable media from computers when not attended.
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal or sensitive information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal or sensitive information contained in documents you fax, copy, scan or print. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment
- Only download personal data from systems if expressly authorised to do so by your manager
- You must not post on the internet personal or sensitive information, or disseminate such information in any way that may compromise its intended restricted audience
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

---

### Storing/Transferring Personal or Sensitive Information Using Removable Media

- Ensure removable media is purchased with encryption.
- Store all removable media securely
- Securely dispose of removable media that may hold personal data
- Use DfE secure access (S2S) for data transfers or encrypt all files containing personal or sensitive data
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean

Please refer to the document on the grid for guidance on How to Encrypt Files

- <http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata>

## **Printing/Scanning/Photocopying**

- All users must ensure that any confidential printed material is not left unattended on photocopiers/printers
- All users to ensure scanned documents are deleted from the hard drive of the photocopier once downloaded

## **Physical Security**

- Visitor identification is always checked
- Visitor badge worn at all times by visitors to school
- Access to areas of school is by permission only
- School site is secured at the beginning and end of each day
- Keys held in locked cupboard
- Keys taken offsite are kept secure by the key holder
- Key register is maintained

## Remote Access

- You are responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access
- To prevent unauthorised access to school systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone
- Select PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment
- No third party will be allowed to access the school system without explicit prior permission. Remote support will be carried out while the member of staff is present.

## Safe Use of Images

---

### Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness. HCC guidance can be found here: <https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf>

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the Headteacher
- Pupils and staff must have permission from the Headteacher before any image can be uploaded for publication

---

### Consent of Adults Who Work at the School

- Permission to use images of all staff who work at the school is sought.

---

### Publishing Pupil's Images and Work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to

the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the school.

Pupils' names will not be published alongside their image and vice versa. Postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only the ICT Manager, Bursar or Clerical Assistant has authority to upload to the internet.

---

## Storage of Images

- Images/ films of children are stored on the school's network and iPads.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resource
- **Mark Taylor** has the responsibility of deleting the images when they are no longer required, or when the pupil has left the school

---

## Surveillance Cameras

- The school uses surveillance cameras for security and safety. The only people with access to this are Headteacher, Bursar and ICT technician. Notification of camera use is displayed at the front of the school. Please refer to the hyperlink below for further guidance <https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf>
  - Cameras on an electronic device which is capable of producing video. School policy should be followed regarding the use of such personal devices
  - Please read in conjunction with the school's CCTV policy.
-

---

## Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school
- All pupils are supervised by a member of staff when video conferencing
- The school keeps a record of video conferences, including date, time and participants
- Approval from the Headteacher is sought prior to all video conferences within school to end-points beyond the school
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences
- No part of any video conference is recorded in any medium without the written consent of those taking part

Additional points to consider:

- Participants in conferences offered by 3<sup>rd</sup> party organisations may not be DBS checked
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference

## School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

---

### School ICT Equipment

- As a user of the school ICT equipment, you are responsible for your activity
- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory
- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available
- Ensure that all ICT equipment that you use is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that you save your data on a frequent basis to the school's network. You are responsible for the backup and restoration of any of your data that is not held on the school's network
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. If it is necessary to do so the local drive must be encrypted
- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles
- Privately owned ICT equipment should not be used on a school network
- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
- All ICT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:
  - maintaining control of the allocation and transfer within their unit
  - recovering and returning equipment when no longer needed
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

---

## Portable & Mobile ICT Equipment

This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight
- Portable equipment must be transported in its protective case if supplied
- When working at home or external environment ensure that paper records are not left unattended and locked away securely when not in use. Do not allow friends of family to view data. Only authorised personnel may use the school ICT equipment.

---

## Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such Smartphones, Blackberries, iPads, games players, are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

### ***Personal Mobile Devices (including phones)***

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device
- Pupils are allowed to bring personal mobile devices/phones to school but these must be handed in to the school office for the duration of the school day. However, pupils are allowed to bring personal mobile devices/phones to school discos that take place termly from 6pm-8.30pm as long as they do not upload any photos taken at the event on social media.
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

### ***School Provided Mobile Devices (including phones)***

- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community
- Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school
- Never use a hand-held mobile phone whilst driving a vehicle

## Telephone Services

- You may make or receive personal telephone calls in designated places, provided:
  1. They are infrequent, kept as brief as possible and do not cause annoyance to others
  2. They are not for profit or to premium rate services
  3. They conform to this and other relevant school policies.
- School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused
- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases
- Ensure that you are available to take any pre-planned incoming telephone calls
- Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat. These procedures should be made readily available throughout your office. If you do not have a copy, please ask the school bursar.

---

## Removable Media

If storing or transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section '**Storing/Transferring Personal or Sensitive Information Using Removable Media**'

- Always consider if an alternative solution already exists
- Only use recommended removable media
- Encrypt and password protect
- Store all removable media securely
- Removable media must be disposed of securely by your ICT support team

## Servers

- Always keep servers in a locked and secure environment
- Limit access rights
- Always password protect and lock the server
- Existing servers should have security software installed appropriate to the machine's specification
- Backup tapes should be encrypted by appropriate software
- Data must be backed up regularly
- Backup tapes/discs must be securely stored in a fireproof container
- Back up media stored off-site must be secure

## Smile and Stay Safe Poster

eSafety guidelines to be displayed throughout the school



**S**taying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

**M**eeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you

**I**nformation online can be untrue, biased or just inaccurate. Someone online may not be telling the truth about who they are - they may not be a 'friend'

**L**et a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online

**E**mails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply

## Social Media, including Facebook and Twitter

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

### Possible Statements

- Our school does not use Facebook and Twitter to communicate with parents and carers
- Staff **are not** permitted to access their personal social media accounts using school equipment at **any time**
- Pupils are not permitted to access social media accounts whilst at school
- Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff, governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever
- Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law

## Systems and Access

- You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC
- Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you
- Ensure you remove portable media from your computer when it is left unattended
- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time
- Do not introduce or propagate viruses
- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or HCC into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)
- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act
- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998
- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a **written guarantee** that they will irretrievably destroy the data by multiple over writing the data.

## Reviewing this Policy

---

### **Review Procedure**

There will be on-going opportunities for staff to discuss with the eSafety coordinator any eSafety issue that concerns them

There will be on-going opportunities for staff to discuss with a member of SLT any issue of data security that concerns them

This policy will be reviewed every (24) months and consideration will be given to the implications for future whole school development planning

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way

This policy has been approved by the full governing body on

## Further help and support

Your organisation has a legal obligation to protect sensitive information under the Data Protection Act 2018. For more information visit the website of the Information Commissioner's Office <https://ico.org.uk/>

Advice on eSafety - <http://www.thegrid.org.uk/eservices/safety/index.shtml>

Further guidance - <http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata>

School's toolkit is available - Record Management Society website – <http://www.rms-gb.org.uk/resources/848>

Test your online safety skills <http://www.getsafeonline.org>

Data Protection Team – email - [dpo@staffordshire.gov.uk](mailto:dpo@staffordshire.gov.uk)

Information Commissioner's Office – [www.ico.org.uk](http://www.ico.org.uk)

Cloud (Educational Apps) Software Services and the Data Protection Act – Departmental advice for local authorities, school leaders, school staff and governing bodies, October 2015. This is an advice and information document issued by the Department for Education. The advice is non-statutory, and has been produced to help recipients understand some of the key principles and their obligations and duties in relation to the Data Protection Act 1998 (the DPA), particularly when considering moving some or all of their software services to internet-based “cloud” service provision – <https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act>

## Current Legislation

---

### Acts Relating to Monitoring of Staff email

#### ***Data Protection Act 2018***

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

<http://www.hmso.gov.uk/acts/acts1998/19980029.htm>

#### ***The Telecommunications (Lawful Business Practice)***

#### ***(Interception of Communications) Regulations 2000***

<http://www.hmso.gov.uk/si/si2000/20002699.htm>

#### ***Regulation of Investigatory Powers Act 2000***

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

<http://www.hmso.gov.uk/acts/acts2000/20000023.htm>

#### ***Human Rights Act 1998***

<http://www.hmso.gov.uk/acts/acts1998/19980042.htm>

---

### Other Acts Relating to eSafety

#### ***Racial and Religious Hatred Act 2006***

It is a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

#### ***Sexual Offences Act 2003***

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.

### ***Communications Act 2003 (section 127)***

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

### ***The Computer Misuse Act 1990 (sections 1 – 3)***

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person's password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

### ***Malicious Communications Act 1988 (section 1)***

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

### ***Copyright, Design and Patents Act 1988***

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining their author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

### ***Public Order Act 1986 (sections 17 – 29)***

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

### ***Protection of Children Act 1978 (Section 1)***

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

## ***Obscene Publications Act 1959 and 1964***

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

## ***Protection from Harassment Act 1997***

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

---

## **Acts Relating to the Protection of Personal Data**

### ***Data Protection Act 2018***

<http://www.legislation.gov.uk/all?title=Data%20Protection%20Act%202018>

### ***The Freedom of Information Act 2000***

<https://ico.org.uk/for-organisations/guide-to-freedom-of-information/>

---

## **Counter-Terrorism and Security Act 2015 (Prevent), Anti-Radicalisation & Counter-Extremism Guidance**

<https://www.gov.uk/government/publications/preventing-extremism-in-schools-and-childrens-services>

## Appendix

### School Policy in Brief

- At this school we have an Acceptable Use policy which is reviewed at least annually, which all staff sign. Copies are kept on file.
- ICT Acceptable Use Agreements are signed by all Staff/ Students/Visitors.
- Safe Handling of Data Guidance documents are issued to all members of the school who have access to sensitive or personal data.

Personal or sensitive material must be encrypted if the material is to be removed from the school

- At this school we use automatically encrypted flash drives for this purpose and limit such data removal.
- At this school we use the DfE S2S site to securely transfer CTF pupil data files to other schools.

Personal or sensitive material must be held in a lockable storage area or cabinet if in an un-encrypted format (such as paper)

- At this school we store such material in lockable storage cabinets in a lockable storage area.
- At this school all servers are in lockable locations and managed by DBS-checked staff.
- At this school we use follow LA back-up procedures and lock the tapes in a fire proof secure cabinet.

Disposal: personal or sensitive material electronic files must be securely overwritten and other media must be shredded, incinerated or otherwise disintegrated for data.

- At this school we use the Authority's recommended current disposal firm for disposal of system hard drives where any protected or restricted data has been held.
- At this school paper based sensitive information is shredded, using cross cut shredders.
- Laptops used by staff at home (loaned by the school) where used for any protected data <are brought in and disposed of through the same procedure.
- SuperUsers with access to setting-up usernames and passwords which enable users to access data systems e.g. for email, network access are controlled by the LA processes and supported by SLT.
- Security policies are reviewed and staff updated at least annually and staff know to whom they should report any incidents where data protection may have been compromised. Staff have guidance documentation.

### Information Security Responsibilities

- DPO – [dpo@staffordshire.gov.uk](mailto:dpo@staffordshire.gov.uk)
- Data Controller – [headteacher@st-josephs-hednesford.staffs.sch.uk](mailto:headteacher@st-josephs-hednesford.staffs.sch.uk)
- Data Processors – all members of salaried school staff.

Governors have a responsibility to ensure effective processes are embedded and carried out effectively.