Our Lady of Lourdes Catholic Primary School

Information Security Framework

July 2019

Our Lady of Lourdes Catholic Primary School
Information Security Framework

Index

Our Lady of Lourdes Catholic Primary School
Information Security Framework

Data Protection

Our Lady of Lourdes Primary School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.
Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Schools also have a duty to issue a Fair Processing Notice to all pupils/parents, this summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

Purpose
This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 2018, General Data Protection Regulations 2018 and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.
All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

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

The Reason for Data Protection
There are many risks involved when it comes to Information Sharing internally and externally. The main risks faced by the school are:

- Safeguarding
- Failure to comply with this policy will have the effect of exposing members of the community, Council staff and the Council itself to risks.
- For members of the public, there is a risk that they may be disadvantaged by uncontrolled releases of their personal information. In extreme cases, members of the public may be put at risk of serious harm.
- Financial
- For the school, failure to comply with the policy carries the risk of substantial fines from the Information Commissioner. Additionally there may be, harm to the school's reputation or in extreme circumstances it may hinder the school from providing vital services.
- Reputational

Non-Compliance with this Information Sharing Guidance
Non-compliance with this Policy may result in significant damage to the school, its reputation, and the interests of its staff and business partners. Any breaches are, therefore, considered to be serious and will be dealt with under the disciplinary process. Third parties in breach of this policy will be dealt with on a case-by-case basis. Employees shall discuss any concerns relating to this Guidance with their line manager.

Data Protection Principles
The Data Protection Act 2018 establishes eight enforceable principles that must be adhered to at all times:
1. Information is to be processed fairly, lawfully and transparently
2. Information is to be used for specified, explicit purposes
3. Information is to be used in a way that is adequate, relevant and limited to only what is necessary
4. Information is accurate and where necessary, kept up to date;
5. Information is kept for no longer than is necessary
6. Information is handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

General Statement
The school is committed to maintaining the above principles at all times. Therefore the school will:

- Inform individuals why the information is being collected when it is collected

- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure our staff are aware of and understand our policies and procedures

Privacy Notices
The GDPR require that we provide privacy notices in simple format to stakeholders. These are in appendix 1.

Subject Access Requests (SAR)

- Subject access request (SAR) – a request made by a data subject for information about, and access to, personal data about themselves that The Organisation is processing, including:
    - a description of the personal data;
    - where/how it is being processed;
    - the purposes for which it is being processed;
    - details of who is allowed to see the personal data;
    - how long it will be kept.

How to recognise a valid Subject Access Request (SAR)
There is no formal way to submit a request. Valid SARs could be sent in writing, including by letter, fax or by electronic means for example: by e-mail, a website form, texts, Facebook or Twitter. They can also be submitted verbally.

They include all requests for personal data, whether or not the data subject has referred to data protection, SARs, the Data Protection Act and include requests which refer to Freedom of Information instead. It is up to you to recognise the request and deal with it as helpfully as possible.

Verbal requests are considered valid, but good practice suggests staff members receiving such requests, should record the details of the request and confirm the details with the requester in order to avoid later disputes. (The request must be documented on the SAR FORM in the appendix 2)

Who can receive a SAR?
A SAR can be given to any member of staff, contracted, permanent or otherwise.

Deadlines
Schools must deal with all reasonable requests within one calendar month, starting on the day after the request is received. Variances to this may include:

- If an identity (ID) check or further information is required to comply with the request, then the deadline will be calculated from the date when the new information is received.
- If the request is deemed complex, the data subject should be informed of the decision and the deadline may be extended by up to two months.

The data subject must also be informed as soon as possible if school holidays could impact the school's ability to carry out ID checks and/or meet the one calendar month deadline.

The SAR procedure
The objective of the procedure is to make sure that the request is properly received and documented and that the nominated Data Protection person can respond to the request in a correct and timely manner.

General staff role:
1. Request is received from a Data Subject.

2. Log the request and inform the relevant people:

2.1. Record the request in the Subject Access Request log:
  2.1.1. Log onto the Data Protection Knowledge Bank at: http://kb.dataprotection.education
  2.1.2. Visit Logs>SAR Logs
  2.1.3. Select your school and click "Add"
  2.1.4. Add the known details as listed in the form, including the date the SAR must be completed. Further details can be added later.
  2.1.5. Click the "Submit" button to save and log the SAR.
2.2. Notify the responsible member of staff (the Data Protection Lead or Headteacher). Data Protection Education will be notified automatically;
2.3. Do this without delay, and within two working days of receipt of the request.
2.4. Updates from both the organisation and Data Protection Education should be added to the existing log online.
2.5. When the SAR is completed, the DPO will mark as closed.

Data protection lead & DPO role

3. The responsible members of staff for dealing with SARs - Data Protection Lead and DPO - qualifies the request and confirms the identity of the data subject.

3.1. If an ID check is needed, the one calendar month deadline starts from when the new information is received.
3.2. If further information to clarify the data request is needed, the one calendar month deadline starts from when the information is received. If the data subject does not provide further clarification, the SAR must still be actioned.

4. If the identity/request is qualified, evaluate the request and compile the requested information:

4.1. The time available under GDPR is one month to provide the information free of charge, unless a request is complex, manifestly unfounded or excessive/repetitive.

5. IF requests are complex, manifestly unfounded or excessive, in particular because they are repetitive, the DPO can decide to:

5.1. For complex requests - extend the time by a further two months (while still notifying the data subject of this decision within one month). In these cases, the most senior level of the organisation will be involved, usually the Governing Board or board of Trustees;
5.2. For excessive/repetitive/unfounded requests - charge a reasonable fee for administrative costs of providing the information; or provide a negative response to the request.

6. Compile and send the requested data, accompanied by the SAR response letter (appendix 3)

6.1. If the request was made electronically (digitally), you should provide the information in a commonly used electronic format.

7. Close the request in the Subject Access Request Log.

Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Contacts

If you have any enquires in relation to this policy, please contact the admin office who will also act as the contact point for any subject access requests.

Our Lady of Lourdes Catholic Primary School
Information Security Framework

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 01625 545745.

Freedom of Information

The governing body is responsible for maintenance of this scheme.

One of the aims of the Freedom of Information Act 2000 (which is referred to as FOIA in the rest of this document) is that public authorities, including all maintained schools, should be clear and proactive about the information they will make public.

The publication scheme covers information already published and information which is to be published in the future.
All information in our publication scheme is available in paper form.
Some information which we hold may not be made public, for example personal information.
This publication scheme conforms to the model scheme for schools approved by the Information Commissioner.

Categories of information published
The publication scheme guides you to information which we currently publish (or have recently published) or which we will publish in the future. This is split into categories of information known as 'classes'. These are contained in section 6 of this scheme.
The classes of information that we undertake to make available are organised into four broad topic areas:
School Information – All relevant and statutory information about the school is published on the school website
Governors' Documents – information published in governing body documents.
Pupils & Curriculum – information about policies that relate to pupils and the school curriculum.
School Policies and other information related to the school - information about policies that relate to the school in general.

How to request information
If you require a paper version of any of the documents within the scheme, please contact the school by telephone, email, fax or letter. Contact details are set out below.
Email: admin@ourladyoflourdes.brighton-hove.sch.uk
Tel: 01273 306980
Contact Address: The Green, Rottingdean, Brighton. BN2 7HA

To help us process your request quickly, please clearly mark any correspondence "PUBLICATION SCHEME REQUEST" (in CAPITALS please)
If the information you are looking for is not available via the scheme you can still contact the school to ask if we have it.

Classes of Information Currently Published (Based on Information Commissioners Office Recommendations)

The table below shows Our Lady of Lourdes Primary School's publication scheme. The scheme covers information already published and information which is to be published in the future. Some information which we hold, such as personal information, may not be made public.

Paying for information
Information published on our website is free, although you may incur costs from your internet service provider. If you don't have internet access, you can access our website using a local library or an internet café. If your request requires a lot of photocopying or printing, or pay a large postage charge or is for a priced item such as some printed publications we will let you know the cost before fulfilling your request. Where there is a charge this will be indicated on the Guide to Information available overleaf.

Our Lady of Lourdes Catholic Primary School
Information Security Framework

Information to be published. **This includes datasets where applicable.**	**How the information can be obtained**	**Cost**
Class 1 - Who we are and what we do (Organisational information, structures, locations and contacts) This will be current information only		
Who's who in the school	Website	free
Who's who on the governing body / board of governors and the basis of their appointment	Website: https://ourladyoflourdesprimaryschool.co.uk/about-us/governors	free
	Hard copy: Contact school	£1
Instrument of Government / Articles of Association	Website: https://ourladyoflourdesprimaryschool.co.uk/about-us/governors	free
	Hard copy: Contact school	£1
Contact details for the governing body, via the school (named contacts where possible).	Website: https://ourladyoflourdesprimaryschool.co.uk/about-us/governors	free
Staffing structure	Website: https://ourladyoflourdesprimaryschool.co.uk/about-us/staff	Free
	Hard copy: Contact school	£1
School session times and term dates	Website: https://ourladyoflourdesprimaryschool.co.uk/information/parents-information/times-of-school-day/ https://ourladyoflourdesprimaryschool.co.uk/information/parents-information/term-times/	Free
	Hard copy: Contact school	£1
Address of school and contact details, including email address.	Website: https://ourladyoflourdesprimaryschool.co.uk/contact-us	Free
Class 2 – What we spend and how we spend it (Financial information relating to projected and actual income and expenditure, procurement, contracts and financial audit) Current and previous financial year as a minimum		
Annual budget plan and financial statements	Hard Copy	£1
Financial audit reports of voluntary funds	Hard copy	£1.50
Procurement and contracts the school has entered into, or information relating to / a link to information held by an	Hard copy	£2

organisation which has done so on its behalf (for example, a local authority or diocese).		
Pay policy	Website	
	Hard copy: Contact school	£2
Governors' allowances that can be incurred or claimed, and a record of total payments made to individual governors.	Website	free
	Hard copy: Contact school	£1.50
Class 3 – What our priorities are and how we are doing (Strategies and plans, performance indicators, audits, inspections and reviews		
School profile	Website: https://ourladyoflourdesprimaryschool.co.uk/about-us	Free
The latest Ofsted report	Website: https://ourladyoflourdesprimaryschool.co.uk/about-us/reports	Free
	Hard copy: Contact school	£1.50
Performance management policy and procedures adopted by the governing body.	Website	free
	Hard copy: Contact school	£2
Performance data or a direct link to it	Website: https://ourladyoflourdesprimaryschool.co.uk/about-us/reports	free
Safeguarding and child protection	Website: https://ourladyoflourdesprimaryschool.co.uk/about-us/policies	Free
	Hard copy: Contact school	£2
Class 4 – How we make decisions (Decision making processes and records of decisions) Current and previous three years as a minimum		
Admissions policy/decisions (not individual admission decisions)	Website: https://ourladyoflourdesprimaryschool.co.uk/home/admissions	Free
	Hard copy: Contact school	£2
Agendas and minutes of meetings of the governing body and its committees. (NB this will exclude information that is properly regarded as private to the meetings).	Website: https://ourladyoflourdesprimaryschool.co.uk/about-us/governors/minutes-of-meetings	Free
	Hard copy: Contact school	Agendas £1 Minutes £2
Class 5 – Our policies and procedures (Current written protocols, policies and procedures for delivering our services and responsibilities) Current information only. As a minimum these must include policies, procedures and		

documents that the school is required to have by statute or by its funding agreement or equivalent, or by the Welsh or English government or the Northern Ireland Executive. These will include policies and procedures for handling information requests. In addition, for Wales, this will include a Welsh Language Scheme in accordance with the Welsh Language Act 1993. For Northern Ireland, this will include an equality scheme / statement in accordance with the Northern Ireland Act 1998.		
Records management and personal data policies, including: • Information security policies • Records retention, destruction and archive policies • Data protection (including information sharing policies)	Website	Free
	Hard copy: contact school	£2
Charging regimes and policies. This should include details of any statutory charging regimes. Charging policies should include charges made for information routinely published. They should clearly state what costs are to be recovered, the basis on which they are made and how they are calculated. If the school charges a fee for re-licensing the use of datasets, it should state in its guide how this is calculated (please see "How to complete the Guide to information").	Charging and Remissions Policy	£2
Class 6 – Lists and Registers Currently maintained lists and registers only (this does not include the attendance register).	(hard copy or website; some information may only be available by inspection)	
Curriculum circulars and statutory instruments ("topic webs")	Website	free
Any information the school is currently legally required to hold in publicly available registers (staff and governor register of interests)	Governor register – website Staff register – hard copy – contact school	Free £1
Class 7 – The services we offer (Information about the services we offer, including leaflets, guidance and newsletters produced for the public and businesses) Current information only	(hard copy or website; some information may only be available by inspection)	
Extra-curricular activities	Website: https://ourladyoflourdesprimaryschool.co.uk/information/parents-information/extra-curricular-activities	Free
Out of school clubs	Website: https://ourladyoflourdesprimaryschool.co.uk/information/parents-information/extra-curricular-activities	Free

Services for which the school is entitled to recover a fee, together with those fees (see Charging and Remissions Policy)	Website Hard copy – contact school	Free £2
School publications, leaflets, books and newsletters	Website: https://ourladyoflourdesprimaryschool.co.uk/news/newsletter-archive	Free
	Hard copy: Contact school	Free

SCHEDULE OF CHARGES

This describes how the charges have been arrived at and should be published as part of the guide.

TYPE OF CHARGE	DESCRIPTION	BASIS OF CHARGE
Disbursement cost	Photocopying/printing @ 0.2p per sheet (black & white)	Actual cost *
	Photocopying/printing @ 2p per sheet (colour)	Actual cost
	Administration cost (staff time)	£15 per hour
	Postage when required	Actual cost of Royal Mail standard 2nd class

* the actual cost incurred by the public authority

Feedback and Complaints
We welcome any comments or suggestions you may have about the scheme. If you want to make any comments about this publication scheme or if you require further assistance or wish to make a complaint then initially this should be addressed to the Headteacher.
If you are not satisfied with the assistance that you get or if we have not been able to resolve your complaint and you feel that a formal complaint needs to be made then this should be addressed to the Information Commissioner's Office. This is the organisation that ensures compliance with the Freedom of Information Act 2000 and that deals with formal complaints. They can be contacted at:
Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
or
Phone: 0303 123 1113 or 01625 545 745
E Mail: casework@ico.org.uk
Website : www.ico.org.uk

Information Sharing Guidance

At Our Lady of Lourdes Primary School, all staff have a responsibility for ensuring appropriate controls and measures around Information Sharing with partner organisations.

General Principles **(to be highlighted to all staff members)**
When sharing information the school is guided by two principles – Can we share the information and Should we share the information. Those are underpinned by the following steps: :

1) Confirm the identity of the person you are sharing with
2) Do not share more information than is necessary
3) Ensure that the information is shared safely and securely
4) Record what information has been shared, where appropriate
5) Check with a manager/DPO or seek advice if you are unsure

Our Lady of Lourdes Catholic Primary School
Information Security Framework

Acceptable Use

The computer system is owned by the school. "The computer system" means all computers and associated equipment belonging to the school, whether part of the school's integrated network or stand-alone, or taken offsite.
Professional use of the computer system is characterised by activities that provide children with appropriate learning experiences, or allow adults to enhance their own professional development or working life. The school recognises that technologies such as the Internet and e-mail will have a profound effect on children's education and staff professional development in the coming years and the school's Internet Access Policy has been drawn up accordingly.
The installation of software or hardware unauthorised by the school, whether legitimately licensed or not is expressly forbidden.
The school reserves the right to examine or delete any files that may be held on its computer systems or to monitor any Internet sites visited.

- All members of staff, students on placement, supply teachers etc. must sign a statement before a system login password is granted.
- All children must be made aware of all the important issues relating to acceptable use, especially the monitoring of Internet use.

Online Safety

The school will appoint an Online Safety Coordinator. This is the Designated Child Protection Coordinator as the roles overlap.
These Online Safety Guidelines have been written by the school, building on government guidance "Teaching Online Safety in School" The school will maintain an active approach to online safety taking into account current guidelines and recommendations from the DfE and similar bodies.
For the purposes of clarity we include in this policy areas which we are current best practice in educational use of information technology.

The importance of Internet use

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet use is part of the national curriculum and a necessary tool for learning.
- Internet access is available for all pupils providing they show a responsible and mature approach to its use. It can be withdrawn if and when misused.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Benefits of the Internet to education

- Benefits of using the Internet in education include:
    - access to world-wide educational resources including museums and art galleries;
    - inclusion in the National Education Network which connects all UK schools;
    - educational and cultural exchanges between pupils world-wide;
    - vocational, social and leisure use in libraries, clubs and at home;
    - access to experts in many fields for pupils and staff;
    - professional development for staff through access to national developments, educational materials and effective curriculum practice;
    - collaboration across support services and professional associations;
    - improved access to technical support including remote management of networks and automatic system updates;
    - exchange of curriculum and administration data with BHCC and DfE;
    - access to learning wherever and whenever convenient.

Using the Internet to enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- We will encourage all pupils, regardless of age, to maintain a sense of their own responsibilities regarding keeping themselves safe and well while using the internet.

Authorisation to use the Internet

- We will maintain a current record of all staff / students who are granted access to the school's electronic communications.
- All staff must read and sign the Information Security Framework before using any school ICT resource.

Evaluation of Internet content

- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Information Systems

Information system security

- Security strategies will be discussed with the Schools' ICT Support team regularly.
- The schools server will be backed up to an offsite location each night
- Anti-Virus protection will be updated regularly.
- The security of individual staff and pupil accounts will be reviewed regularly.
- The administrator account password will be changed if it becomes known to unauthorised persons.
- Computers (including mobile devices) may not be connected to the school network both physically or wirelessly without specific permission.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Portable media may not be used to take data off site without specific permission.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files will not be moved or removed from a shared folder without specific permission.
- Personal data will not be stored on school servers without specific permission. Files held on the school's network will be regularly checked.
- Software will not be installed/removed from computers without specific permission.
- The ICT co-ordinator / network manager will review system capacity regularly.

E-mail

- All school business may only be conducted via an approved school email account.
- E-mail sent to external organisations should be written carefully and where appropriate, authorised before sending, in the same way as a letter written on school headed paper.

Encrypted E-mail

During the course of its activities, the school and the employees may have need or be required to send sensitive information via e-mail. If this occurs, all employees will follow the guidelines set out in our General Principles.

All employees will use encrypted email to send any type of sensitive information.

Management of published content

- The contact details on the website are the school address, e-mail and telephone number. Staff or pupils' personal information must not be published without their consent (ie photos).
- The head teacher, in collaboration with admin staff, will take overall editorial responsibility and ensure that content is accurate and appropriate.

- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.
- Pupils will be taught the reasons for caution in publishing personal information and images in social networking and media sites

Management of social networking and personal publishing

- The school will block/filter access to social networking sites. Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils are advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice will be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school.
- Teachers' official blogs or wikis should be password protected or include a membership requirement and run from the school website. Teachers are advised not to run social network spaces for student use on a personal basis.
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils will be encouraged to invite known friends only and deny access to others.
- Pupils should be advised not to publish specific and detailed private thoughts.
- Pupils will be made aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

For additional information, see Social Media Guidelines below.

Web Filtering

- We will work with our IT support to ensure that systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL must be reported to the e-Safety Coordinator.
- Along with IT support, senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Our filtering strategy will be designed by SLT to suit the age and curriculum requirements of the pupils, advised by IT support.Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.
- Those responsible for managing filtering systems or monitoring ICT use will have clear procedures for reporting issues.

Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Mobile Phones

- Mobile phones will not be used during lessons or formal school time.
- The sending of abusive or inappropriate text messages is forbidden.
- Mobile phones will be kept by the school office during the school day.

Risk Assessment

- We will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor IT support can accept liability for the material accessed, or any consequences resulting from Internet use.
- We will monitor breaches of this policy and, if necessary, conduct a review of our E-Safety procedures to ensure they are adequate and their implementation appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence.
- We will work with IT support to gain assurance that methods to identify, assess and minimise risks are reviewed regularly.

E-safety complaints procedure
Parents and pupils will need to work in partnership with staff to resolve issues.

- Complaints regarding Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Pupils and parents will be informed of the complaints procedure.

Staff training

- Staff training in safe and responsible Internet use and on school e-Safety Procedures will be provided when deemed necessary by SLT.

Parental involvement
A partnership approach with parents will be encouraged.

- Parents' attention will be drawn to this document using a variety of means.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- Interested parents may be referred to other organisations

Removable Media Guidelines

No removable media is to be used within school or on school-based computer systems to store or transfer sensitive information or data.

Non-sensitive/non-confidential data may be brought into school using removable media, ie by visitors for a presentation or assembly.

Where a user has a defined need to use removable media to take non-sensitive or non-confidential data off the school system, the requirement should be documented and be approved by the Headteacher, using the form in appendix 4.

All computers in the school should be restricted to "read only" access to portable media except for devices held in secure rooms such as the Headteacher's and SENCo office. The Headteacher will inform the IT service provider of these excepted devices.

Home Working Guidelines

For many, the nature of working in a school predicates home working. Where this is undertaken all employees will follow the same guidelines as they would if working in school.

All employees must be trained in the use of Microsoft One-Drive, which ensures a secure approach to accessing documents etc. through an online / cloud-based server.

Remote access to the school systems is secured by VPN, and no data must be copied off the school network onto personal devices, unless following the Removable Media Guidelines.

Images

Image taking by parents, legal guardians or family members

- Parents, legal guardians, family members and friends can take images - using camera, phone or other device - of their child and friends participating in school activities for family and personal use (this does not include school trips). These must not be uploaded to social media where other children may be accidentally or intentionally viewed.
- Parents/carers will be asked for their permission before photography is allowed.
- Before they are allowed to take images during school activities, parents or legal guardians have to sign an agreement that any images they take will not be used inappropriately, This agreement is undertaken on signing in to the school building.
- Photography and video filming will be limited to designated areas.
- Use of cameras and other equipment will be monitored.

Images for school publications:

- Images that include pupils will be selected carefully, and pupils' full names will not be used anywhere on the website.
- Parents / carers have the choice to opt in to their children having their photographs used by the school
- Children should be made aware of why their picture is being taken and how it will be used e.g. Headteacher Award and photo placed in Newsletter.
- The consent form should encourage parents/carers to recognise the value of group photographs or recordings of school events.
- Images will be kept securely and held by the school for the duration of the pupil's time there, after which they will be destroyed or they may be kept for archiving purposes for the public interest.
- Images of children from the school will not be used to illustrate controversial subjects, as determined by the governing body
- Written permission from the school should be obtained before pupils or parents/carers publish images taken from the school website or of school events.

Images for the school website/social media pages:

- School websites and social media pages are part of the internet and are more easily accessible than paper based school publications. The school will make sure that only appropriate images are used. Image filenames will avoid using children's names.

Webcams:

- Webcams are a useful tool for learning. They can allow an individual or class to interact over the internet with others and support links between pupils in different schools, countries and cultures.
- A webcam will only be used in appropriate circumstances such as a normal class setting.
- Both children and teachers will be made aware of when a webcam is in use.

Children photographing one another:

- Staff will supervise and maintain control over any photographing pupils do during on-school or off-site activities e.g. photos taken on residential trips.
- The use of personal phones or devices with photographic capability will not be permitted during school hours in any area of the school or on external or residential trips by children unless agreed by the Headteacher.
- A school / class camera will be used during school trips; children will not be permitted to bring personal mobile / smart phones or devices with photographic capability.
- If it is found that cameras or camera phones have been misused, the school will follow its usual disciplinary procedures.

Please note that images taken by the media are not covered by this policy and are subject to a separate set of regulations by the media regulatory bodies, such as Ofcom and the Independent Press Standards Association.

All parents / carers have the right to withdraw their children from any form of photography or video imaging being taken but must inform the school in writing of this decision (Appendix 5)

Social Media Guidelines

Staff Use of Social Media

School staff's social media profiles should not be available to pupils / ex-pupils. If they have a personal profile on social media sites, they should reconsider using their full name, as pupils / ex-pupils may be able to find them. Staff should consider using a first and middle name instead, and set public profiles to private.

Moreover, staff should not attempt to contact pupils / ex-pupils or their parents via social media, or any other means outside school, in order to develop any sort of relationship. They will not make any efforts to find pupils' / ex-pupils' or parents' social media profiles.

Staff will ensure that they do not post any images online that identify children who are pupils / ex-pupils at the school.

Parental use of Social Media & Social Networking Policy

Social networking sites such as Facebook and Twitter are now widely used. This type of media allows people to communicate in ways that were not previously possible. However, such sites can be inappropriately used by some as a means of expressing negative or offensive views about schools and their staff. This document sets out Our Lady of Lourdes Primary School's approach to parental/carer use of such sites and sets out the procedures we will follow and action we may take when we consider that parents have used such facilities inappropriately. When we have referred to "parent" in this document, we also include carers; relatives; or anyone associated with the School.

Objectives

The purpose of this document is to:

- Clarify what the School considers appropriate and inappropriate use of social networking sites by parents
- Encourage social networking sites to be used in a beneficial and positive way by parents
- Safeguard pupils, staff and anyone associated with the school from the negative effects of social networking sites
- Safeguard the reputation of the School from unwarranted abuse on social networking sites
- Set out the procedures the School will follow where it considers parents have inappropriately or unlawfully used social networking sites to the detriment of the School, its staff or its pupils, and anyone else associated with the School
- Set out the action the School will consider taking if parents make inappropriate use of social networking sites

Appropriate use of social networking sites by parents

Social networking sites have potential to enhance the learning and achievement of pupils, enable parents to access information about the School, and provide feedback efficiently and easily. In addition, the School recognises that many parents and other family members will have personal social networking accounts, which they might use to discuss/share views about school issues with friends and acquaintances. As a guide, individuals should consider the following prior to posting any information on social networking sites about the School, its staff, its pupils, or anyone else associated with the School:

- Is the social networking site the appropriate channel to raise concerns, give this feedback or express these views?
- Would private and confidential discussions with the School be more appropriate? E.g. if there are serious allegations being made/concerns being raised. Social media/internet sites should not be used to name individuals and make abusive comments about those people. Please contact the school directly to discuss any concerns you may have.
- Are such comments likely to cause emotional or reputational harm to individuals that would not be justified, particularly if the School has not yet had a chance to investigate a complaint?
- The reputational impact that the posting of such material may have to the School; any detrimental harm that the School may suffer because of the posting; and the impact that such a posting may have on pupils' learning.

Inappropriate use of social networking sites by parents

Although social networking sites may appear to be the quickest and easiest way to express frustrations or concerns about the School (and those associated with it), it is rarely appropriate to do so. Other channels, such as a private and confidential discussion with the School, or using the School's formal complaints process are much better suited to this. The School considers the following examples to be inappropriate uses of social networking sites. This is not an exhaustive list and is intended to provide examples only:

- Making allegations about staff or pupils at the School
- Cyber-bullying

- Making complaints about the School/staff at the School
- Making defamatory statements about the School or staff at the School
- Posting negative/offensive comments about specific pupils/staff at the School
- Posting racist/homophobic/sexist/prejudicial or discriminatory comments
- Posting comments that threaten violence
- Making negative comments about other parents

Parents should also ensure that their children are not using social networking/internet sites in an inappropriate manner. It is expected that parents/carers explain to their children what is acceptable to post online. Parents/carers are also expected to monitor their children's online activity, including in relation to their use of social media keeping in mind there are age-limits to many of these sites.

Procedure the School will follow if inappropriate use continues
The School will always try to deal with concerns raised by parents in a professional and appropriate manner and understands that parents may not always realise when they have used social networking sites inappropriately. Therefore, as a first step, the School will usually discuss the matter with the parent to try to resolve the matter and to ask that the relevant information be removed from the social networking site in question. If the parent refuses to do this and continues to use social networking sites in a manner the School considers inappropriate, the School will consider taking the following action:

- Take legal advice and/or legal action where the information posted is defamatory in any way or if the circumstances warrant this
- Set out the School's concerns to you in writing, giving you a warning and requesting that the material in question be removed
- Contact the Police where the School feels it appropriate – for example, if it considers a crime (such as harassment) has been committed or in cases where the posting has a racial element, is considered to be grossly obscene or is threatening violence
- If the inappropriate comments have been made on a school website or online forum, the School may take action to block or restrict that individual's access to that website or forum
- Contact the host/provider of the Social Networking site to complain about the content of the site and ask for removal of the information
- Take other legal action against the individual.

Data Loss / Breach Guidelines

This procedure applies in the event of a personal data breach under Article 33 Notification of a personal data breach to the supervisory authority, and Article 34 Communication of a personal data breach to the data subject of the General Data Protection Regulation (GDPR).

Simply put, the procedure applies to all data breaches including computer security incidents as defined and explained below.

The GDPR introduced a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority (The ICO). This must be done within 72 hours of becoming aware of the breach, where feasible:

- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, individuals must also be informed without undue delay;
- Organisations should ensure they have robust breach detection, investigation and internal reporting procedures in place. This will facilitate the decision to notify the ICO and/or the affected individuals;
- Organisations must also keep a record of any personal data breaches, regardless of whether they require notification to the ICO.

Our Lady of Lourdes Catholic Primary School
Information Security Framework

Who

This procedure applies to **all staff and managers** (whether employees, contractors or temporary staff) of Our Lady of Lourdes Catholic Primary School

- Everyone is required to be aware of, and to follow this procedure in the event of a personal data breach;
- The Organisation's Data Protection Officer (DPO)/Data Protection Lead and other managers/IT service desk as appropriate - have responsibilities to contain/restore the data breach and assess the risks to individuals;
- The Data Protection Officer - will notify the ICO of the breach within 72 hours and will inform all Data Subjects that have been compromised in any Data Breach, where required to do so;
- Training Lead – will ensure training is provided to ensure all staff are aware of this procedure and how to find/implement it.

Definitions

The Organisation – Our Lady of Lourdes Catholic Primary School is the school or establishment acting as a Data Controller which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Personal data - Any information relating to an identified or identifiable living person ('data subject') i.e. someone who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to information regarding the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Data breach - The accidental or unlawful loss, destruction, alteration or unauthorised disclosure of personal data that can occur for many reasons, from IT failures through to human error. They can fall into one or more of these categories:

- **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, personal data;
- **Integrity breach** - where there is an unauthorised or accidental alteration of personal data;
- **Availability breach** - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

Examples of data breaches

- Loss or theft of paper records or loss or theft of equipment on which data is stored e.g. laptop, mobile phone, tablet device, memory stick;
- Letter or email containing personal and/or confidential data sent to the wrong address or an email to unauthorised group email boxes;
- Personal data disclosed orally in error in a meeting or over the phone – including 'blagging' where information is obtained by deceiving The Organisation, or where information has been disclosed without confirming the true identity of the requester;
- Unauthorised access to information classified as personal or confidential e.g. attaching documents to an outlook diary appointment that is openly accessible;

- Posting information on the world wide web or on a computer otherwise accessible from the Internet without proper information security precautions;
- Sensitive information left on the photo-copier or on a desk in County Council premises;
- Unauthorised alteration or deletion of information;
- Not storing personal and confidential information securely;
- Not ensuring the proper transfer or destruction of files after closure of offices/buildings e.g. not following building decommissioning procedures;
- Failure to safeguard/remove personal data on office equipment (including computers and smart phones) before disposal/sale.

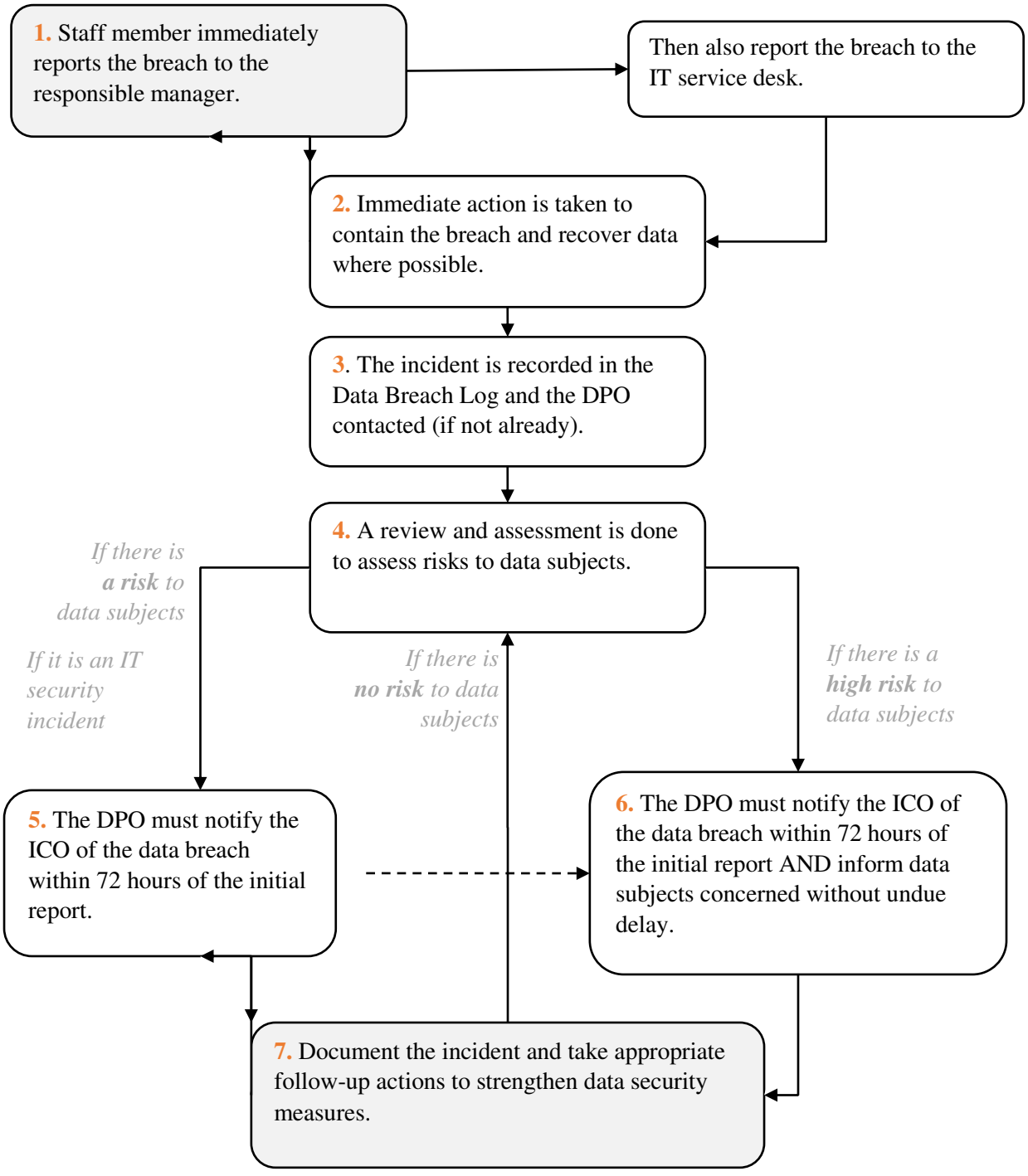
Example data breaches caused by IT Security Incidents

- Unauthorised access to the IT systems because of misconfigured and/or inappropriate access controls;
- Hacking or phishing attack and related suspicious activity;
- Virus or malware attacks and related suspicious activity;
- ICT infrastructure-generated suspicious activity;
- Divulging a password to another user without authority.

Our Lady of Lourdes Catholic Primary School
Information Security Framework

Procedure Overview

When a member of staff detects or suspects a potential personal data breach:



Our Lady of Lourdes Catholic Primary School
Information Security Framework

Personal data breach procedure steps

1. Reporting the data breach
Anyone who detects or suspects a personal data breach or an IT security incident, must report it immediately!

- ***Report to*** the responsible manager or DPO
- If the breach is related to an IT security incident, ***also report to*** **the IT service desk**

2. Contain the breach and recover data
The responsible manager/DPO must take immediate action to contain the breach and to recover any information disclosed or lost.

3. Record the incident in the Data Breach Log
This step needs to be done straight away. Once any immediate damage is contained, the responsible manager/DPO needs to record a detailed description of the breach in the Data Breach Log and inform the DPO/data protection lead if they are not already involved.

The type of information that should be recorded initially (and after the incident review and risk assessment) includes:

- A description of the nature of the breach;
- The number of data subjects and personal data records affected;
- The categories of personal/sensitive data affected;
- Likely consequences of the breach;
- Any measures that have been or will be taken to address/mitigate the breach.

To record the breach in the online data breach log:

i. Log onto the Data Protection Knowledge Bank at: http://kb.dataprotection.education
ii. Visit Logs>Breach Logs
iii. Select your school and click “Add”
iv. Add the known details as listed in the form. Further details can be added later.
v. Click the “Submit” button to save and log the Breach log
vi. DPE will be informed automatically.
vii. All updates to the log will be sent to DPE and the listed school manager
viii. When the issue is completed, the DPO will close the breach log

4. Incident review and risk assessment
The GDPR gives the following explanation of possible risks and consequences related to a data breach:

“A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.”

The risk assessment (RA) must be carried out straight away to establish what personal/sensitive data was involved in the breach and to determine the likelihood and severity of the resulting risk to those concerned. It should also outline what data protection precautions have been taken and any further actions needed.

4.1 Criteria for notification and justification
The output of the risk assessment will decide the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen (again).

- If there is **no risk** to data subjects e.g. the incident involves encrypted data for which there is another existing source, then the DPO doesn't have to notify the ICO or data subjects but needs to justify this decision in the documentation;
- If there **is a risk** to data subjects, the DPO must notify the ICO as soon as possible and within 72 hours;
- If there a **high risk*** to data subjects, then those concerned must also be informed directly and without undue delay.
  * If the impact of the breach is assessed as more severe, the risk is higher; if the likelihood of the consequences is greater, then the risk is higher.

5. Notifying the ICO
The DPO must notify the ICO within 72 hours of the breach and provide the information as mentioned below. (If this is not all available, the ICO should be notified and advised when any additional information will be provided).

Notification is made by **email.**

Confirmation of receipt of this information is made by **email.**

The information sent to the ICO contains a description of the personal data breach including, where possible:

- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (DPO) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

6. Notifying the data subjects
The DPO will promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them as follows:

- The breach must be described in clear and plain language including the nature of the personal data breach and similar information as supplied to the ICO, as a minimum:
  - the name and contact details of your data protection officer or other contact point where more information can be obtained;
  - a description of the likely consequences of the personal data breach; and
  - a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, the measures taken to mitigate any possible adverse effects.

7. Appropriate actions and documentation
The DPO/Organisation must complete its document on the incident and monitor/document the appropriate follow-up actions taken to strengthen data security measures. This type of record keeping is key to the school demonstrating 'accountability' for data protection in line with the GDPR legislation.

Our Lady of Lourdes Catholic Primary School
Information Security Framework

Appendix 1 – Privacy Notices

Staff Privacy Notice

Data Controller
Our Lady of Lourdes RC Primary School complies with the GDPR and is registered as a 'Data Controller' with the Information Commissioner's Office (Reg. No. Z1631331).

The Data Protection Officer (DPO) services for the school are provided by Data Protection Education, 1 Saltmore Farm, New Inn Road, Hinxworth, Baldock, SG7 5EZ.

We ensure that your personal data is processed fairly and lawfully, is accurate, is kept secure and is retained for no longer than is necessary.

The Legal Basis for Processing Personal Data
We process personal data because it is necessary in order to comply with the School's legal obligations and to enable it to perform tasks carried out in the public interest.

Special Category data processing is carried out in the public interest and is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law and, when necessary, to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

How we use information
We process personal data relating to those we employ to work at, or otherwise engage to work at our School.

- This is for employment purposes, to assist in the running of the School and/or to enable individuals to be paid.

The collection of this information will benefit both national and local users by:

- improving the management of workforce data across the sector
- enabling development of a comprehensive picture of the workforce and how it is deployed
- informing the development of recruitment and retention policies
- allowing better financial modelling and planning
- enabling ethnicity and disability monitoring
- supporting the work of the School Teachers' Review Body
- protecting vulnerable individuals
- the prevention and detection of crime

This personal data includes some or all of the following - identifiers such as name and National Insurance Number and characteristics such as ethnic group; employment contract and remuneration details, qualifications, information relevant to the School Work Force Census and absence information.

Who we share data with
We routinely share data with:

- workplaces or volunteer placements that staff attend either whilst working with us or after leaving us
- the local authority (Human Resources and Payroll)
- the Department for Education (DfE)

- third parties working in school (e.g. catering companies or organisations running after school clubs)
- software providers (e.g. where we use software for the purposes running the school)
- agencies with whom we have a duty to co-operate (e.g. Emergency and Social Services)

We will not give information about you to anyone outside the School without your consent unless the law allows us to.

Retention Periods
Personal data will not be retained by the School for longer than necessary in relation to the purposes for which they were collected.

Information will be held in accordance with the Information and Records Management Society Tool Kit for Schools.

https://irms.site-ym.com/page/SchoolsToolkit

Rights
You have the right to:

1. be informed of data processing (which is covered by this Privacy Notice)
2. access information (also known as a Subject Access Request)
3. have inaccuracies corrected
4. have information erased
5. restrict processing
6. data portability
7. intervention in respect of automated decision making
8. withdraw consent (see below)
9. complain to the Information Commissioner's Office (See below)

To exercise any of these rights please contact the DPO.

Withdrawal of Consent
Where the School processes personal data solely on the basis that you have consented to the processing, you will have the right to withdraw that consent.

Complaints to ICO
If you are unhappy with the way your request has been handled, you may wish to ask for a review of our decision by contacting the DPO.
If you are not content with the outcome of the internal review, you may apply directly to the Information Commissioner for a decision. Generally, the ICO cannot make a decision unless you have exhausted our internal review procedure. The Information Commissioner can be contacted at:

The Information Commissioner's Office,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire
SK9 5AF.

Our Lady of Lourdes Catholic Primary School
Information Security Framework

Pupil Privacy Notice

Data Controller
Our Lady of Lourdes RC Primary School complies with the GDPR and is registered as a 'Data Controller' with the Information Commissioner's Office (Reg. No. Z1631331).

The Data Protection Officer (DPO) services for the school are provided by Data Protection Education, 1 Saltmore Farm, New Inn Road, Hinxworth, Baldock, SG7 5EZ.

We ensure that your personal data is processed fairly and lawfully, is accurate, is kept secure and is retained for no longer than is necessary.

The Legal Basis for Processing Personal Data
We process personal data because it is necessary in order to comply with the schools legal obligations and to enable it to perform tasks carried out in the public interest.

Special Category data processing is carried out in the public interest and is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law and, when necessary, to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

How we use information
We collect and hold personal information relating to our pupils and those involved in their care, we may also receive information from previous schools, the local authority(s) and/or the Department for Education (DfE). We use this personal data to:

- support our pupils' learning
- support our pupils' welfare
- monitor and report on their progress
- provide appropriate pastoral care
- assess the quality of our services
- process any complaints
- protecting vulnerable individuals
- the prevention and detection of crime

This information will include a child's Unique Pupil Number (UPN), contact details, carers details, national curriculum assessment results, examination results, attendance information, any exclusion information, where they go after they leave us and personal characteristics such as their ethnic group, any special educational needs or disabilities they may have as well as relevant medical information.

Who we share data with
We routinely share data with:

- schools that pupils attend after leaving us
- the Local Authority (Education and Social Services)
- the Department for Education (DfE)
- health visitors, school nurse or Primary Care Trust (PCT)

- third parties working in school (e.g. catering companies who need pupil allergy information or organisations running after school clubs)
- software providers (e.g. where we use software for the purposes of tracking attainment or behaviour)
- agencies with whom we have a duty to co-operate (e.g. Emergency and other Enforcement Agencies)

Retention Periods
Personal data will not be retained by the school for longer than necessary in relation to the purposes for which they were collected.

Information will be held in accordance with the Information and Records Management Society Tool Kit for Schools.

https://irms.site-ym.com/page/SchoolsToolkit

Photographs
The School may take photographs, videos or webcam recordings of pupils or students for official use, monitoring and for educational purposes. You will be made aware that this is happening and the context in which the photograph will be used.

Photographs may also be taken of those attending a ceremony which may appear in the newspaper. You will be made aware that this is happening and the context in which the photograph will be used.

Rights
You have the right to:

1. be informed of data processing (which is covered by this Privacy Notice)
2. access information (also known as a Subject Access Request)
3. have inaccuracies corrected
4. have information erased
5. restrict processing
6. data portability
7. intervention in respect of automated decision making
8. withdraw consent (see below)
9. complain to the Information Commissioner's Office (See below)

To exercise any of these rights please contact the DPO

Withdrawal of Consent
Where the school processes personal data solely on the basis that you have consented to the processing, you will have the right to withdraw that consent.

Complaints to ICO
If you are unhappy with the way your request has been handled, you may wish to ask for a review of our decision by contacting the DPO.

If you are not content with the outcome of the internal review, you may apply directly to the Information Commissioner for a decision. Generally, the ICO cannot make a decision unless you have exhausted our internal review procedure. The Information Commissioner can be contacted at:

The Information Commissioner's Office,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire
SK9 5AF.

Our Lady of Lourdes Catholic Primary School
Information Security Framework

Governors' Privacy Notice

Data Controller
Our Lady of Lourdes RC Primary School complies with the GDPR and is registered as a 'Data Controller' with the Information Commissioner's Office (Reg. No. Z1631331).

The Data Protection Officer (DPO) services for the school are provided by Data Protection Education, 1 Saltmore Farm, New Inn Road, Hinxworth, Baldock, SG7 5EZ.

We ensure that your personal data is processed fairly and lawfully, is accurate, is kept secure and is retained for no longer than is necessary.

The Legal Basis for Processing Personal Data
We process personal data because it is necessary in order to comply with the School's legal obligations and to enable it to perform tasks carried out in the public interest.

Special Category data processing is carried out in the public interest and is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law and, when necessary, to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

How we use information
We process personal data relating to those who govern at our School.

- This is essential, in order for the school to fulfil their official functions and meet legal requirements

We use this data to:

- Meet the statutory duties placed upon us
- Facilitate communication with members of the governing body
- Assist governors in exercising their duties

This personal data includes name, contact details and date of birth.

Who we share data with
We routinely share data with:

- The Local Authority – We are required to share information about our governors with our local authority (LA) under the Education Act 1996. If you require more information about how the local authority store your personal data, please visit https://www.brighton-hove.gov.uk/content/council-and-democracy/about-your-council/data-protection
- The Department for Education - The Department for Education (DfE) collects personal data from educational settings and local authorities. We are required to share information about our governors with the Department for Education (DfE) under section 538 of the Education Act 1996
- The National Governance Association – The Governing Body subscribes to this organisation. Their publications supply governors with relevant information which assists them in exercising their duties.

We will not give information about you to anyone outside the School without your consent unless the law allows us to.

Retention Periods
Personal data will not be retained for longer than necessary in relation to the purposes for which they were collected.

Information will be held in accordance with the Information and Records Management Society Tool Kit for Schools.

https://irms.site-ym.com/page/SchoolsToolkit

Rights
You have the right to:

1. be informed of data processing (which is covered by this Privacy Notice)
2. access information (also known as a Subject Access Request)
3. have inaccuracies corrected
4. have information erased
5. restrict processing
6. data portability
7. intervention in respect of automated decision making
8. withdraw consent (see below)
9. complain to the Information Commissioner's Office (See below)

To exercise any of these rights please contact the DPO.

Withdrawal of Consent
Where the School processes personal data solely on the basis that you have consented to the processing, you will have the right to withdraw that consent.

Complaints to ICO
If you are unhappy with the way your request has been handled, you may wish to ask for a review of our decision by contacting the DPO.

If you are not content with the outcome of the internal review, you may apply directly to the Information Commissioner for a decision. Generally, the ICO cannot make a decision unless you have exhausted our internal review procedure. The Information Commissioner can be contacted at:

The Information Commissioner's Office,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire
SK9 5AF.

Our Lady of Lourdes Catholic Primary School
Information Security Framework

Appendix 2 – SAR Request Form

SUBJECT ACCESS REQUEST (FORM) – PART 1

By completing this form, you are making a subject access request under the General Data Protection Regulation (GDPR) for personal information held about you by Our Lady of Lourdes Catholic Primary School that you are eligible to receive. Please complete this form and return it to Our Lady of Lourdes Catholic Primary School.

A) The Data Subject Details

Title	
Surname	
First Name(s)	
Current Address	
Telephone (Home)	
Telephone (Work)	
Telephone (Mobile)	
Email address	
Date of birth	
Details of identification provided to confirm name of data subject in question	
Details of data requested: *[Example: Emails between "A" and "B" from 1 May 2017 to 6 September 2017.]*	

B) Declaration of Data Subject

By signing below, you indicate that you are the individual named above. The organisation cannot accept requests regarding your personal data from anyone else including family members – see Part 2. We may need to contact you for further identifying information before responding to your request. You warrant that you are the individual named and will fully indemnify us for all losses and expenses if you are not.

Signature: …… Date: ……

Our Lady of Lourdes Catholic Primary School
Information Security Framework

SUBJECT ACCESS REQUEST (FORM) – PART 2

C) Declaration of behalf of Data Subject

If you are requesting the information on behalf of a data subject, please complete this section:

Are you acting on behalf of the data subject with their written consent or in another legal authority?	Yes	No
If 'Yes' please state your relationship with the data subject (e.g. parent, legal guardian or solicitor)		
Has proof been provided to confirm you are legally authorised to obtain the information?	Yes	No

Title	
Surname	
First Name(s)	
Current Address	
Telephone (Home)	
Telephone (Work)	
Telephone (Mobile)	
Email address	

I hereby request that Our Lady of Lourdes Catholic Primary School provide me with the information about the data subject above.

Name ……

Signature: ……

Date: ……

Our Lady of Lourdes Catholic Primary School
Information Security Framework

Appendix 3 – SAR Response Letter

[Name]

[Address]

[Date]

Dear [Name of data subject]

Thank you for your letter of [date] making a data subject access request. We have processed this request under the Data Protection Act 2018.

Your request was as follows:

[Edit to reflect the nature of the request e.g.]

Please could I therefore have a copy of all my personal data including but not limited to:

- **Any information held by xxx (e.g. xxx cited some examples about my appraisal in a notebook from her note book)**
- **Any letters / emails issued to staff or governors or volunteers that contained personal data about me**
- **Any emails between staff referencing me that I wasn't copied in on**
- **Any information on my performance or behaviours**

This request is in four parts:

- **Any information held by xxx (e.g. xxx cited some examples about my appraisal in a notebook from her note book)**

Your response along the lines of "We are pleased to enclose the information you requested". Or ''We are unable to provide this information because [justification here]''. But consider whether you have this information, whether you are the data controller and whether providing the information would require the consent of the individual.

- **Any letters / emails issued to staff or governors or volunteers that contained personal data about me**

Your response along the lines of "We are pleased to enclose the information you requested". Or "We are unable to provide this information because [justification here]".

- **Any emails between staff referencing me that I wasn't copied in on**

Your response along the lines of "We are pleased to enclose the information you requested". Or "We are unable to provide this information because [justification here]". I would provide these but redact any references to third-parties

- **Any information on my performance or behaviours**

Your response along the lines of "We are pleased to enclose the information you requested". Or "We are unable to provide this information because [justification here]". Consider the Management Information exemption if necessary.

Regards, [Name]

[Responder's Name

Contact Details]

Your rights

If you are unhappy with the way your request for information has been handled, you can request a review within the next 40 working days by writing to *[suggest your contact or Chair of Governors – or the Data Protection Officer once the paperwork is done!]*

If, having exhausted our review procedure, you remain dissatisfied with the handling of your request or complaint, you will have a right to appeal to the Information Commissioner at: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF (telephone: 0303 123 1113; website www.ico.org.uk). There is no charge for making an appeal.

Our Lady of Lourdes Catholic Primary School
Information Security Framework

Appendix 4: Removable Media Approval Form

Removable Media Guidelines

No removable media is to be used within school or on school-based computer systems to store or transfer sensitive information or data.

The risk associated with not implementing or adhering to this policy is threefold:

1. The confidentiality of information may be compromised.
2. Copyright, or Intellectual Property Rights infringement may be facilitated.
3. Malicious software may be introduced to school Systems.

Where a user has a defined need to use removable media, the requirement should be documented and be approved by the Headteacher below:

Name of User	
Reason for requirement to use removable media	
Additional Notes	
We understand the risks associated with the use of removable media as outlined above and believe that the reason for the requirement outlined above warrant these risks.	
Signature Headteacher	
Signature User	

Appendix 5 – Photo Consent Withdrawal Form

Our Lady of Lourdes Catholic Primary School

Photographs and Video Consent Withdrawal Form

I wish to withdraw all previous consent granted for any purpose of my child's photographs and video.

I understand that a new consent form must be completed in order to provide consent for any specific purpose or use of photographs and video.

I understand that images taken and published prior to this and any future publication of these images will remain available as our policy.

I have read and understood the information above.

Pupil Name	
Name of parent/carer	
Signature of parent/carer	
Date:	