Purley Partnership Federation

Purley Nursery School
Achieving and growing together

Christ Church Primary School
Nurturing lifelong learners with God's guidance

General Data Protection Regulation & Freedom of Information Policy

Rewritten April 2018, review April 2021

Contents

Data Protection Policy

To function properly the schools need to collect and use certain types of information about staff, pupils and other individuals who come into contact with the schools in order to operate. The schools are legally obliged, under the General Data Protection Regulation (GDPR) 2018, to protect all information and ensure that it is processed fairly, lawfully and in a transparent manner.

'Processing' includes the obtaining, holding, use or disclosure of that information.

The schools must only collect information that they need for specific, explicit and legitimate purposes. They must:

- keep it secure;
- ensure it is relevant, accurate and up to date;
- only hold as much information as needed;
- use it only in a way that is adequate, relevant and limited;
- keep it no longer than necessary;
- process the information in a manner that ensures appropriate security of the personal data;
- allow the subject of the information to see it on request.

Why protect information?

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

What information do you need to protect?

You should secure any personal data you hold about individuals and any data that is deemed sensitive or valuable to the schools.

Data as defined under the Regulation may include both facts and opinions about individuals. It also includes information regarding the intentions of the data controller (ie the schools) towards the individual or who else might be using the data (data processors).

Article 4 (1) of GDPR defines **personal data** as being:

- *'Any information relating to an identified or identifiable natural person'*
- *'An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, generic, mental, economic, cultural or social identity of that natural person'*

The GDPR addresses the export of personal data to outside of the EU and also includes IP addresses, biometric data, mobile device IDs, cookies on websites, etc.

The Designated Protection Officer (DPO), overseen by the Executive Head Teacher/Head of School, has the specific responsibility for Data Protection within each school.
The schools have designated the Deputy Head Teacher of Christ Church School and the Lead Teacher of Purley Nursery School as the people responsible for working out exactly what information needs to be secured. The DPO for each school needs to understand what information is handled, how the information changes over time, who else is able to use it and why.

The DPO for each school ensures that everyone managing and handling personal information:

- understands that they are contractually responsible for following good data protection practice,
- is appropriately trained to do so,
- is appropriately supervised,
- knows that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against the members of staff concerned.

ALL STAFF have a shared responsibility to secure any sensitive or personal data used in their day-to-day professional duties.
The Governors, Executive Head Teacher, Head of School and the DPOs ensure that as part of the process of regularly reviewing this policy every three years that:

- a review and audit is made of the way personal information is held, managed and used annually,
- methods of handling personal information are assessed and evaluated annually,
- performance with handling personal information is assessed and evaluated annually.

School Data Security

All Staff and Governors within Christ Church C of E Primary School and Purley Nursery School will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. Some **guidance is given in the 'Dos and Don'ts' appendix** but this is not exhaustive and all staff should make sure that they act, at all times, in line with the principles of the GDPR.

What happens if the Act is breached?

The school that the breach has occurred within must undertake an investigation of the breach and where necessary, refer the breach to the Information Commissioner's Office (ICO). Both the school and individuals may be liable for breaches of the Regulation. Each school will have a 'Breach Log' to monitor and record any breaches. Criminal offences carry fines with a current maximum of 20 million Euros or 4% of global annual turnover for serious breaches of the Regulation or on conviction of indictment, an unlimited fine.

A breach of the Regulation can also lead to serious reputational damage; the ICO publishes a press release on its website where breaches of the Regulation occur.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the General Data Protection Regulation 2018. In case of any queries or questions in relation to this policy please contact the relevant school's DPO.

Data sharing

Both schools also have a duty to act in the best interest of the child and will share any concerns or worries that may be disclosed to the appropriate bodies, as necessary.

In the process of carrying out their ~~its~~ core functions the schools may on occasions need to share a pupil's personal data with third parties (e.g. an Educational Psychologist).

The schools will only share personal data if it is in compliance with the Principles of the GDPR. The amount of information shared, and the extent of sharing, will be limited to that necessary to carry out a particular function.

Staff, parents and pupils of the schools have rights around their personal data. These are:

- the right to be informed
- the right of access to their data
- the right to rectify data
- the right to their data being erased when no longer at the school
- the right to restrict processing (unless it will restrict the level of education and teaching)
- the right to data portability
- the right to object to how personal data is used
- rights around the decision making or profiling of data

Under the new Regulations the parents can request to see copies of the personal data the schools store on themselves or on their child. Requests should be made to the applicable school's DPO in writing. The schools have 1 month from the request date to gather the personal information that has been requested. If this request comes in over a school holiday, the schools can discuss suitable timescales with the requestor.

Time period over which data is held

Both schools adhere to the principle that they will only hold as much data as needed, and only for as long as it is needed. Please see the Purley Partnership Federation Retention Policy for further information.

Note that pupil paper records are either delivered by hand or sent recorded delivery to their new school when they leave. Electronic records are sent through secure email to the next school at the same time.

Both schools have the right to hold data on a pupil that allows them to effectively teach the pupil.

This policy should be read in conjunction with the:

- Data security ‘Dos and Don’ts’ (Appendix 1 to this policy)
- Data Retention Policy
- Code of Conduct
- Child Protection Policy
- School Teachers Pay and Conditions Document
- Equal Opportunities and Race Equality Policy
- SEND Policy
- Monitoring and Evaluation Policy
- General Data Protection Regulation (2018)
- Parent, Staff and Pupil Privacy Notices for the Purley Partnership Federation

Freedom of Information Policy

One of the aims of the Freedom of Information Act 2000 (FOI) is that public authorities, including all maintained schools, should be clear and proactive about the information they will make public.

This scheme sets out:

- the classes of information which we publish;
- the manner in which the information will be published; and
- whether the information is available free of charge or on payment.

The scheme covers information already published. All information in our publication scheme is either available for you on each schools' website to download and print off or 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). This is split into categories of information known as 'classes'. These are contained below.

The classes of information that we undertake to make available are organised into four broad topic areas:

- *School Profile and other information relating to the governing body* – information published in the School Profile and in other 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 schools in general.

How to request information

If you require a paper version of any of the documents within the scheme, please contact the relevant school by telephone, email, fax or letter. Contact details are set out below, or you can visit the applicable school's website at www.christchurch.croydon.sch.uk or www.purleynurseryschoolcc.com

Email:	office1@christchurch.croydon.sch.uk (Christ Church School) office@purley.croydon.sch.uk (Purley Nursery School)
Tel:	020 8660 7500 (Christ Church School) 020 8660 5639 (Purley Nursery School)
Contact Address:	Christ Church C of E Primary School, Montpelier Road, Purley. CR8 2QE Purley Nursery School, 58 Pampisford Road, Purley. CR8 2NE

To help us process your request quickly, please clearly mark any correspondence **"PUBLICATION SCHEME REQUEST**" (in CAPITALS please).

If the information you're looking for isn't available via the scheme and isn't on our websites, you can still contact the applicable school to ask if we have it.

Paying for information

Information published on our websites is free, although you may incur costs from your Internet service provider. If you don't have Internet access, you can access our websites using a local library or an Internet café.

Single copies of information covered by this publication are provided free unless stated otherwise. If your request means that we have to do a lot of photocopying or printing, or pay a large postage charge, or is for a priced item such as some printed publications or videos we will let you know the cost before fulfilling your request. Where there is a charge this will be indicated by a £ sign in the description box.

Back to top

Classes of Information Currently Published

School Profile and other information relating to the Governing Body - this section sets out information published in the Schools' Profiles and in other Governing Body documents.

Class	Description
School Brochure	There is no longer a statutory requirement to produce an annual prospectus or have a curriculum policy, to avoid duplication of effort and unnecessary cost. Maintained schools, Academies and Free Schools are required to publish specified information online (from September 2012), so that parents have the information they need to make informed decisions about their child's education. Christ Church school and Purley Nursery School make their policy information available on the school website including a school brochure.
Instrument of Government	● The name of the school/s ● The category of the school/s ● The name of the governing body ● The manner in which the governing body is constituted ● The term of office of each category of governor if less than 4 years ● The name of any body entitled to appoint any category of governor ● Details of any trust ● If the school/s has a religious character, a description of the ethos ● The date the instrument takes effect
Minutes [1] of meetings of the governing body and its committees	Agreed minutes of meetings of the governing body and its committees *[current and last full academic school year]*

[1] Some information might be confidential or otherwise exempt from the publication by law – we cannot therefore publish this

Pupils & Curriculum Policies - This section gives access to information about policies that relate to pupils and the school curriculum.

Class	Description
Home school agreement	Statement of each school's aims and values, their responsibilities, the parental responsibilities and the expectations of its pupils, for example home-learning arrangements.
Curriculum subject policies	Statement on policies for curriculum subjects and religious education and schemes of work and syllabuses currently used by the school/s.
Sex Relationship Education Policy	Statement of policy with regard to sex and relationship education.
Special Education Needs and Disability Policy and Inclusion statement	Information about the policy on providing for pupils with special educational needs.
Equalities and Community Cohesion Policy (including Equalities Statement)	Statement of policy for promoting equal opportunities including race, gender and disability equality. This also includes the plan for increasing participation of disabled pupils in the schools' curriculum, improving the accessibility of the physical environment and improving delivery of information to disabled pupils.
Collective Worship	Statement of arrangements for the required daily act of collective worship.
Child Protection and Safeguarding Policy	Statement of policy for safeguarding and promoting welfare of pupils at the schools.
Behaviour and discipline statement	Statement of general principles on behaviour and discipline.
Behaviour, discipline & anti-bullying policy	Describes measures taken by the schools to maintain good behaviour and to prevent bullying.
Exceptionally Able Learners	Information about the policy on providing for pupils who are exceptionally able learners.

School Policies and other information related to each school - This section gives access to information about policies that relate to the schools in general.

Class	Description
Published reports of Ofsted referring expressly to the schools	Published report of the last inspection of the schools and, where appropriate, inspection reports of religious education in those schools designated as having a religious character.
Ofsted inspection Self-Evaluation Form[2]	A statement of the Governing Body's evaluation of the schools' performance.
School session times and term dates	Details of school session and dates of school terms and holidays.
Health and Safety Policy and risk assessments	Statement of general policy with respect to health and safety at work of employees (and others) and the organisation and arrangements for carrying out the policy.
Complaints procedure	Statement of procedures for dealing with complaints.
Appraisal of Staff	Statement of procedures adopted by the governing body relating to the performance management of staff and the annual report of the Executive Head Teacher and the Head of School on the effectiveness of appraisal procedures.
Code of Conduct	Statement of procedure for regulating conduct and discipline of school staff and procedures by which staff may seek redress for grievance.
Pay Policy	Statement of the pay policy regarding staff pay including procedures for determining staff grievances in relation to their pay.
Curriculum circulars and statutory instruments	Any statutory instruments, departmental circulars and administrative memoranda sent by the Department of Education and Skills to the Executive Head Teacher, Head of School or governing body relating to the curriculum.
Admissions Policy	Statement of the policy on admissions.

Information of the school policies can be found on each school's website:
www.christchurch.croydon.sch.uk
www.purleynurseryschoolcc.com

[2] Some information might be confidential or otherwise exempt from the publication by law – we cannot therefore publish this

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 either the Executive Head Teacher of Christ Church C of E Primary School, Montpelier Road, Purley, CR8 2Q or the Head of School of Purley Nursery, 58 Pampisford Road, Purley. CR8 2NE

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

Enquiry/Information Line: 01625 545 700
E Mail: publications@ic-foi.demon.co.uk
Website: www.informationcommissioner.gov.uk
Back to top

Appendix 1

Data security - dos and don'ts
September 2019

This policy is drawn from BECTA guidance issued in Jan 2009 for anyone working in school who collects, manages, transfers or uses data about learners, staff or other individuals during the course of their work.
The Becta website closed in July 2011 but the source of this information has been archived and can be found at the following link
http://webarchive.nationalarchives.gov.uk/20110130111510/http:/schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_mis_im03&rid=14734

Aim

To raise your awareness of where potential breaches of security could occur.

Data Breaches under GDPR

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. The schools must do this 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, we must also inform those individuals without undue delay.

We endeavour to ensure that we have a robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.

We keep a record of any personal data breaches, regardless of whether we notify the ICO of the breach.

Dos and Don'ts

Following these will help to prevent data from being lost or used in a way which may cause individuals harm or distress and/or prevent the loss of reputation the schools may suffer if personal data about individuals is lost.

Your roles and responsibilities

As a member of your organisation you have a shared responsibility to secure any sensitive or personal data you use in your day-to-day professional duties.

Important 'Do's'

- Make sure you and your colleagues are adequately trained.
- Follow current guidance.
- Become more security aware.
- Raise any security concerns.

- Store data in accordance with the policies and training.
- Encourage your colleagues to follow good practice and guidance.
- Report incidents.

Steps you can take to help prevent security problems

There are plenty of things that you should do (or not do) that will greatly reduce the risks of sensitive information going missing or being obtained illegally. Many of these 'dos and don'ts' will apply to how you handle your own personal information. Using these practices will help you to protect your own privacy.

We have separated these points into different areas to make it easier for you to refer back to.

Working online:

Do

- Make sure that you keep any computers you use at home where you work on sensitive data up to date. Computers need regular updates to their operating systems, web browsers and security software (anti-virus and anti-spyware).
- Only visit websites on the school laptops that are allowed by the schools.
- Remember the schools may monitor and record (log) the websites you visit.
- Turn on relevant security warnings in your web browser (for example, the automatic phishing filter available in Internet Explorer and attack and forgery site warnings in Mozilla Firefox).
- Make sure that you only install software that the IT team has checked and approved.
- Be wary of links to websites in emails, especially if the email is unsolicited.
- Only download files or programs from sources you trust. If in doubt, talk to the IT team.
- Check that your organisation has an acceptable-use policy (AUP)[3] for the internet and ensure that you follow it.

Email and messaging:

Do

- Report any spam or phishing[4] emails to the IT team that are not blocked or filtered.
- Report phishing emails to the organisation they are supposedly from.
- Use your organisation's contacts or address book. This helps to stop emails being sent to the wrong address.

Don't:

[3] This is found within our E-safety policy.

[4] Phishing is an attempt to obtain your personal information (for example, account details) by sending you an email that appears to be from a trusted source (for example, your bank) [http://www.google.co.uk/search?q=define%3A+phishing].

- Click on links in unsolicited emails. Be especially wary of emails requesting or asking you to confirm any personal information, such as passwords, bank details and so on.
- Turn off any email security measures that your IT team has put in place or recommended.
- Email sensitive information unless you know it is encrypted[5]. Talk to your IT team for advice.
- Reply to chain emails.
- Use personal email accounts for school matters. This is prohibited.

Passwords:
Do

- Use a strong password (strong passwords are usually eight characters or more and contain upper and lower case letters, as well as numbers or symbols).
- Make your password easy to remember, but hard to guess.
- Choose a password that is quick to type.
- Use a mnemonic (such as a rhyme, acronym or phrase) to help you remember your password.
- Change your password(s) if you think someone may have found out what they are.

Don't:

- Share your passwords with anyone else except the IT team.
- Write your passwords down – *but you can use the secure store on LGfL – see Appendix 2*.
- Use your work passwords for your own personal online accounts.
- Save passwords in web browsers if offered to do so.
- Use your username as a password.
- Use names as passwords.
- Email your password or share it in an instant message.

Laptops:
Do

- Shut down your laptop using the 'Shut Down' or 'Turn Off' option when going home.
- Turn on the lock screen when leaving the laptop unattended.
- Try to prevent people from watching you enter passwords or view sensitive information.
- Turn off and store your laptop securely (if travelling, use your hotel's safe).
- Use a physical laptop lock if available to prevent theft.
- Lock your desktop when leaving your laptop unattended.

Don't:

[5] Encryption is a way of scrambling information. It helps stop anyone using the information if they do not have an electronic key or password to unscramble it.

- Save personal data to your laptop. Personal data should either be encrypted, saved to the network or to an encrypted stick.
- Store remote access information with your laptop.
- Leave your laptop unattended unless you trust the physical security in place.
- Use public wireless hotspots – they are not secure.
- Leave your laptop in your car. If this is unavoidable, temporarily lock it out of sight in the boot.
- Let unauthorised people use your laptop.
- Let a supply teacher use your laptop unless logged on with the supply user name.
- Don't leave your laptop or PC in presenter mode when unattended*. In school when your computer goes onto standby you need a password to bring your computer off standby. This is not the case for home and office PCs which should be locked when away from your desk.*

Sending and sharing:

Do

- Be aware of who you are allowed to share information with. Check with your Information Asset Owner if you are not sure.
- Ask third parties how they will protect sensitive information once it has been passed to them.
- Encrypt all removable media (USB pen drives, CDs, portable drives) taken outside the schools that contains any form of information classes as personal on an individual or sent by post or courier.
- Use the staff area or the network for sharing documents with school staff. For example ASPs can be found in the SENCO folder of the staff area of the school network.
- Use Google Drive for documents that other staff might need access to.
- Use USO-FX to send confidential information to colleagues in school (see Appendix 3), other Croydon Schools or the LEA or password protect the document you are going to send by clicking on the file tab and selecting 'permissions' and 'encrypt with password'.

Don't

- Send sensitive information by email unless it is encrypted.
- Send sensitive information (even if encrypted) on removable media (USB pen drives, CDs, portable drives) if secure remote access is available.
- Place protective labels on outside envelopes. Use an inner envelope if necessary. This means that people can't see from the outside that the envelope contains sensitive information.
- Assume that third-party organisations know how your information should be protected.
- Refer to a child by name in an e-mail, use initials or "the child we were discussing this morning".
- Attach documents that detail about the child or an individual without password protecting the document.

Working on-site:

Do

- Make sure that you put sensitive information away when left unattended.
- Shred any confidential paperwork.

Don't

- Position screens or class information documents where they can be read from outside the room.
- Put confidential documents in non-confidential recycling bins.
- Print off reports with personal data (eg pupil data) unless absolutely necessary.
- Use unencrypted memory sticks for any data that is classed as personal.
- Leave personal information unclaimed on any printer.

Working off-site:
Do

- Only take offsite information you are authorised to and only when it is necessary. Ensure that it is protected offsite in the ways referred to above.
- Ensure that all paper-based information that is taken off-site is kept confidential and secure, ideally in an envelope which indicates the return address if misplaced.
- Wherever possible access data remotely using Google Drive instead of taking it off-site.
- Be aware of your location and take appropriate action to reduce the risk of theft. Particular care should be taken in public places (eg reading of documentation on public transport).
- Make sure you sign out completely from any services you have used.
- Try to reduce the risk of people looking at what you are working with.
- Leave your laptop behind if you travel abroad (some countries restrict or prohibit encryption technologies).

Do not

- Take confidential information to an entertainment or public place such as a pub or cinema, whether held on paper or an electronic device. Any information must be taken to the destination directly and never left unattended during the journey.
- Leave documentation in vehicles overnight.
- Discuss case level issues at social events or in public places.

Further help and support

Your organisation has a legal obligation to protect personal information. Your senior management should be aware of their legal obligations under the General Data Protection Regulations 2018. For more information, visit the website of the Information Commissioner's Office [http://www.ico.gov.uk].

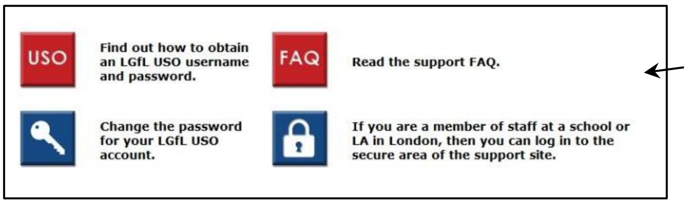
Back to top

Appendix 2

Using the secure password store (Christ Church School)

Log onto LGfL (link from Christ Church website)

Choose "Log into the Support site"



USO Find out how to obtain an LGfL USO username and password.

FAQ Read the support FAQ.

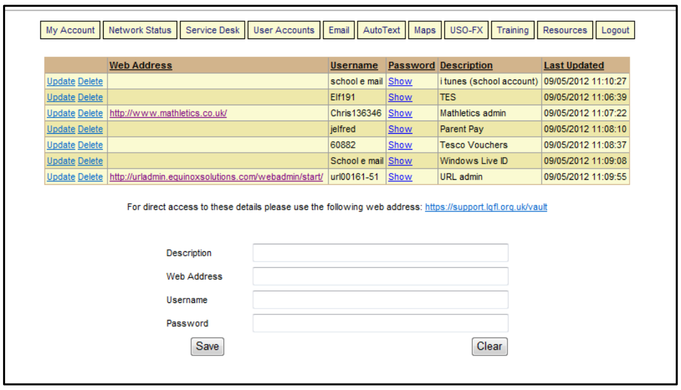
Change the password for your LGfL USO account.

If you are a member of staff at a school or LA in London, then you can log in to the secure area of the support site.

Choose the blue padlock and use your USO and password to log on

Go to "My Account" and choose USO Password Vault

You can save your passwords here.



	Web Address	Username	Password	Description	Last Updated
Update Delete		school e mail	Show	i tunes (school account)	09/05/2012 11:10:27
Update Delete		Elf191	Show	TES	09/05/2012 11:06:39
Update Delete	http://www.mathletics.co.uk/	Chris136346	Show	Mathletics admin	09/05/2012 11:07:22
Update Delete		jelfred	Show	Parent Pay	09/05/2012 11:08:10
Update Delete		60882	Show	Tesco Vouchers	09/05/2012 11:08:37
Update Delete		School e mail	Show	Windows Live ID	09/05/2012 11:09:08
Update Delete	http://urladmin.equinoxsolutions.com/webadmin/start/	url00161-51	Show	URL admin	09/05/2012 11:09:55

For direct access to these details please use the following web address: https://support.lgfl.org.uk/vault

Description

Web Address

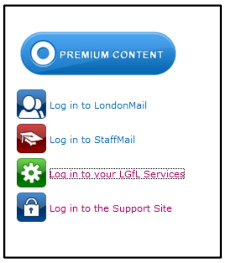
Username

Password

Back to top

Appendix 3

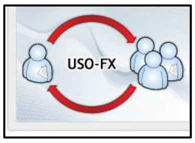
Transferring documents securely (Christ Church School)



Log onto LGfL (link from Christ Church website)

Choose "Log into your LGfL Services"

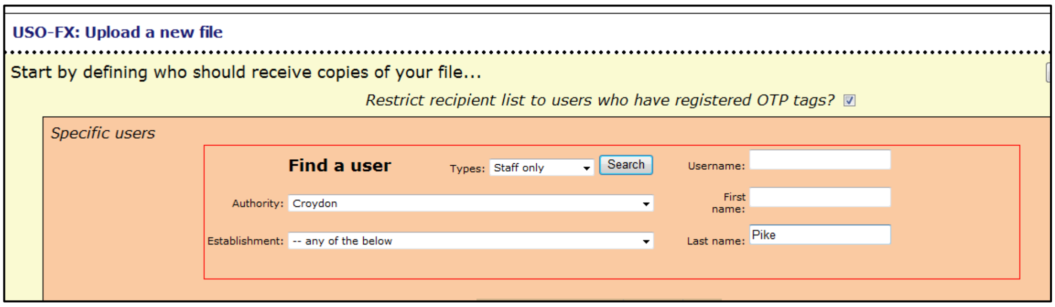
Use your USO and password to log on



Choose USO-FX

Choose "upload a file"

Take the tick out of the box "Restrict recipient list to users who have registered OTP tags"



USO-FX: Upload a new file

Start by defining who should receive copies of your file...

Restrict recipient list to users who have registered OTP tags? ☑

Specific users

Find a user

Types: Staff only

Username:

Authority: Croydon

First name:

Establishment: -- any of the below

Last name: Pike

the surname here and click 'Search'

Select your recipient from the list and then either click "add" to add another user or click "next" to upload your document.

Click Next again and then use the next window to give your message a title eg John Smith's ASP and then upload your document. You can only upload one document at a time.

Click finish.

Back to top

Appendix 4

Data Protection Breach Form

Name of person reporting breach: ________________________________

Date: ____________________

Name of person responsible for the breach (if known):

____

Category of Breach (please tick):

Type of breach	**Tick**
(Accidental) destruction of data	
Loss or theft of items/devices storing data	
(Accidental) alteration of the data – human error	
Unauthorised disclosure of or access to personal data	
Hacking	
Data obtained by deception	
Unforeseen circumstances – fire, flood etc	
Other (please state)	

Please provide more details about the breach (how and when, what data was involved, steps taken already):

Action taken, when and by whom (including details on containment/recovery, assessing on-going risk, notification, evaluation):

DPO – Anne Hudson

Back to top