HIGH WELL SCHOOL
Preparing for Positive Futures

General Data Protection Regulation

Inc. Publication Scheme, Privacy Notice, Freedom of Information Requests and COVID-19 (Appropriate Policy Document) Special Category

Policy Lead:	Business Manager
Date approved by Governing Body:	31.01.2022
Date Shared with Staff:	07.02.2022
Date of Review:	January 2023

Signed by Chair of Governors:	Margaret Turner
Date:	31.01.2022

Contents

1. Introduction

High Well School is committed to the protection, fair and proper use of all information regarding individuals who come into contact with the school. This policy is intended to ensure that the handling of personal and sensitive data will be in line with the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018.

The GDPR is part of the fundamental right to privacy and the law applies to any 'processing of personal data'. The UK data protection regime is set out in the DPA 2018 and the GDPR (which also forms part of UK law) Guide to the GDPR.

- **Processing** includes collecting, recording, storing, using, analysing, combining, disclosing or deleting data.

- **Data controller** – Wakefield Council is the data controller for High Well School and will decide how and why to collect and use the data. They will ensure that the processing of that data complies with data protection law.

- **A processor** is a separate person or organisation (not an employee) who processes data on behalf of the controller and in accordance with their instructions. Processors have some direct legal obligations, but these are more limited than the controller's obligations.

- **A data subject –** is the individual whom the particular personal data is about

- **The Information Commissioners Office (ICO)** - is the supervisory authority for data protection in the UK. They offer advice and guidance, promote good practice, monitor breach reports, conduct audits, consider complaints, monitor compliance and take enforcement action where appropriate. https://ico.org.uk/

The legal bases for processing data are as follows –

(a) Consent: the member of staff/pupil/parent has given clear consent for the school to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for the member of staff's employment contract or pupil placement contract.

(c) Legal obligation: the processing is necessary for the school to comply with the law (not including contractual obligations)

The members of staff responsible for data protection are mainly the Headteacher, School Business Manager and School Business Support Officer. However it is imperative that all staff treat all pupil information in a confidential manner and follow the guidelines as set out in this document.

The school is committed to ensuring that its staff are aware of GDPR and the legal requirements and adequate training is provided to them.

The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

2. Personal and Sensitive Data

'Personal data' is information that identifies an individual, and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain. This may include their race or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; physical or mental health; an individual's sexual orientation etc.

All data within High Well school's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

3. The Data Protection Principles

The following data protection principles of the GDPR shall be applied to all data processed:

- Ensuring that data is fairly and lawfully processed;
- Processing data only for limited purposes;
- Ensuring that all data processed is adequate, relevant and not excessive;
- Ensuring that data processed is accurate;
- Not keeping data longer than is necessary;
- Ensuring that data is secure.

4. Fair Processing / Privacy Notice

High Well School will be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and pupils prior to the processing of individual's data. Notifications shall be in accordance with ICO guidance https://ico.org.uk/your-data-matters/your-right-to-be-informed-if-your-personal-data-is-being-used/

All parents and pupils will be sent a copy of the School's Privacy Notice which is located at Appendix 1 of this policy. This Privacy Notice will also be published on the website.

There may be circumstances where the school is required either by law or in the best interests of our pupils or staff to pass information onto external authorities, for example local authorities, Ofsted, or the Department of Health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation or individual outside of our school shall be clearly defined within notifications and details of the basis for sharing given. This data will only be shared if it is relevant information to their external job role or a prior request for the data has been

cleared by the Data Manager in school is namely the School Business Manager. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

Any proposed change to the processing of individual's data shall first be notified to them.

Under no circumstances will the school disclose information or data:

- that would cause serious harm to the child or anyone else's physical or mental health or condition;
- indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child;
- recorded by the pupil in an examination that would allow another person to be identified or identifies another person as the source, unless the person is an employee of the school or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed;
- in the form of a reference given to another school or any other place of education and training, the child's potential employer, or any national body concerned with pupil admissions.

5. Data Security

High Well School will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this Policy and their duties under the GDPR.

High Well School will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

6. Notification

High Well School's data processing activities will be registered with the Information Commissioner's Office (ICO). Details are available from https://ico.org.uk/

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

Breaches of personal or sensitive data shall be notified within 72 hours to the individual(s) concerned and the ICO.

7. Data Access Requests (Subject Access Requests)

All individuals whose data is held by High Well School have a legal right to request access to such data or information about what is held.

High Well School shall respond to such requests **within one month** of receipt of request however this time limit may be extended by **a further two months** if the request is complex or if the school receives a number of requests from the individual.

Requests for data should be made in writing to:

Headteacher
High Well School
Rookhill Road
Pontefract
WF8 2DD

No charge will be applied to process the request.

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. Data may be disclosed to the following third parties without consent:

- **Other schools**
  If a pupil transfers from High Well School to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school via the DFE's Schools information transfer system via Common Transfer Files which are heavily encrypted. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.

  Child Protection files will be either delivered in person to the new setting of via recorded and signed for delivery.

- **Examination authorities**
  This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

- **Health authorities**
  As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

- **Police and courts**
  If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

- **Social workers and support agencies**
  In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

- **Educational division**
  Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

- **Right to erasure:**
  Where any personal data is no longer required for its original purpose, an individual can request that the processing is stopped and all their personal data is erased by the school including any data held by contracted processors.

8. Photographs and Video

Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in school only.

Unless prior consent from parents/pupils/staff has been given, the school shall not utilise such images for publication or communication to external sources.

It is the school's policy that external parties (including parents) may not capture images of staff or pupils during such activities without prior consent.

All CCTV footage is automatically overwritten after 31 days.

The school operate a learning platform called Iris Connect which records lessons, this is used solely for staff training and class auditing purposes and is not shown to any external parties. This may be used with parental permission to ask for external professionals to provide advice eg Education Psychology, Learning Support etc.

9. Location of Information and Data

Hard copy data, records, and personal information are stored out of sight and in a locked cabinet. The only exception to this is medical information that may require immediate access during the school day. This will be stored on School Pod.

Sensitive or personal information and data should not be removed from the school site, however the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with pupils.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.

- Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.

- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.

- If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.

- If it is necessary to transport data away from the school, it should be downloaded onto a USB stick. The data should not be transferred from this stick onto any home or public computers. Work should be edited from the USB, and saved onto the USB only.
- USB sticks that staff use must be encrypted and password protected. The use of these will be phased out due to a new encrypted server being installed.

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

10. Data Disposal

The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements. This is also an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

Disposal of IT assets holding data shall be in compliance with ICO guidance: https://ico.org.uk/media/fororganisations/documents/1570/it_asset_disposal_for_organisations.pdf and should:

- ensure that the responsibility of asset disposal is assigned to a member of High Well staff with a suitable level of authority (in partnership with Alamo IT Services);
- complete a full inventory of all equipment that has been marked for disposal;
- be clear about what will happen with devices when the item is no longer needed;
- consider the security vulnerabilities associated with each method of disposal;
- ensure personal data is deleted before recycling devices, so that data is not accessible to others after the device has left High Well School's ownership;

- be aware that any specialist service provider used will be considered to be a 'data processor' under the DPA;
- have a written contract in place between High Well School and the data processor (Alamo IT Services) ensuring that there is an appropriate level of security in place.

The school has identified a qualified source for disposal of IT assets and collections.
The school also uses Russell Richardson who conform to ISO 9001 and BS8470 regulation standards.to dispose of sensitive data that is no longer required.

Data Controller: High Well School
Data Protection Officer: School Business Manager
Data Processor: Administration Staff

Appendix 1

Publications Scheme

Who we are and what we do

High Well is a special school for seventy pupils aged between 11-16 years with an Education, Health and Care Plan for Profound/Severe Social, Emotional and Mental Health Needs (SEMH). At High Well we aim to prepare every pupil for a positive future. Our core purpose is to develop our pupils' academic, social and emotional skills so that each pupil leaves us ready and equipped for further education, employment or training, knows how to keep themselves safe, and is able to contribute to society.

Many of our pupils come to us having experienced disruption to their school life, often from an early age. At High Well we aim to provide stability and consistency for both pupils and parents/carers in order to overcome barriers to learning through supporting and teaching our pupils how to manage and regulate their emotions and feelings. Thorough and robust assessment ensures that we identify what each pupil already knows and where there are any gaps in their learning/development. This allows us to plan to meet individual pupils' needs and ensure that every pupil makes good or better progress.

For a list of our staff team, please visit our website at:
https://www.highwellschool.org.uk/page/?title=Staff+Team%26%23160%3B&pid=14

Constitution and legal governance

High Well School is a maintained school of Wakefield Council. Our Governing Body are responsible for making sure the school provides a good quality education for all pupils. They are accountable to parents, the local community and the Local Authority.

The Governing Board:

- is accountable for the performance of the school to parents and the wider community
- plans the school's future direction
- selects the head teacher
- makes decisions on the school's budget and staffing including the performance management policy
- makes sure the agreed Curriculum is well taught
- decides how the school can encourage pupils' spiritual, moral and cultural development

For a list of our Governing Body, please visit our website at:
https://www.highwellschool.org.uk/page/?title=Governors&pid=17

What we spend and how we spend it
High Well School receives income from the Local Authority including Pupil Premium, Government Dedicated Schools Grant and Capital monies.

The Governing Body is accountable for the way I which the school's resources are allocated and Governors need to secure the best possible outcome for pupils, in the most efficient and effective way, at a reasonable cost.

Governors, the Headteacher and School Business Manager have developed and work to procedures for assessing need, and obtaining goods and services which provide value for money in terms of suitability, efficiency, time, and cost. Measures in place include:

- obtaining three quotes for orders above £3,000
- a competitive tendering procedures for goods and services over £75,000 in accordance with LA regulations as detailed in the Wakefield Scheme for Financing Schools.

High Well School's finances is closely monitored by the Local Authority Finance Department by: reviews, financial health checks, benchmarking exercises and the Schools Financial Value Standard self-assessment.

For further information on our Financial Management, please see our Financial Management Policy situated on the website under 'Policies'.

What our priorities are and how we are doing

High Well School's Strategic Priorities for 2021 – 2025 are as follows:

- All pupils leave with the skills, experience and confidence to succeed Post-16 and in adulthood.
- Across all Key Stages, pupils achieve the best possible outcomes compared to their starting points.
- To excel at partnerships, developing strong and effective relationships, leading to excellent outcomes for pupils and their families.
- To become an emotional wellbeing centre of excellence, and are a happy, healthy and resilient school community.
- To use research to develop expertise in pedagogy for SEMH and associated SEND resulting in excellent outcomes for our pupils.

Leadership and Management

- Build the capacity of new leaders so they are better able to improve the quality of teaching and ensure all pupils achieve good outcomes
- Provide training for key members of staff in Mental Health First Aid and emotional wellbeing support to provide a layer of support for staff ensuring staff are emotionally resilient to meet the complex needs of pupils.
- Develop leadership capacity to ensure responsibility for improvement is distributed across the school and provide opportunities to grow the next stage of senior leaders

Progress towards achieving the above priorities is monitored by the Leadership Team on a monthly basis and by the Governing Body on a termly basis.

Ofsted
We were last inspected by Ofsted in May 2017 and were graded 'Good'.

Our policies and procedures
High Well School have the following policies and procedures which are situated on the website:

Accessibility Allegations against Staff Anti-Bribery and Fraud Anti-Bullying Appraisal – Teacher and Support Staff Attendance Behaviour Principles in School Capability of Staff Careers Advice Charging and Remissions Complaints Designated Teacher – LAC Discipline, Conduct and Grievance Emergency Planning Equality and Diversity External Visits Financial Management First Aid GDPR and Subject Access Requests	Governor's Equality Health and Safety Induction Invacuation and Lockdown Lone Working NQT Online Safety Pay Premises Management Pupil and Staff Death Policy (inc. Bereavement) Recruitment Safeguarding SEND Sex Education Supporting Pupils with Medicines Teachers Pay Training Whistleblowing Worship - Religion

Lists and registers

We collect pupil information via registration forms at the start of the school year and / or Common Transfer File or secure file transfer from previous school. This pupil data is essential for the school's operating use.

We use a 'School Pod' system which holds information on contact information for pupils and staff (including emergency contacts), absences, incidents, safeguarding, attendance, exclusions, behaviour and a communication record with parents/carers.

We use an Inventry sign in system for all staff and visitors to sign in when entering and leaving the building for security and Health and Safety.

We keep a Single Central Record and HR files on all staff, governors and contractors. This record is the central record of the safeguarding checks that have been carried out on staff and other relevant people. The files also contain information on training attended.

We hold all financial records on all income and expenditure, petty cash imprest account, payment card information, staff pay, staff mileage and overtime, school meals and school uniform financial information.

Appendix 2

Freedom of Information Requests

How to make a request

The Freedom of Information Act gives you the right to ask to see or be provided with a copy of any information that any public body holds.

You need to make a request to us in writing.

You can email the Business Manager at: businessmangager@highwell.org.uk for information held by us of write to:

Business Manager
High Well School
Rookwell Road
Pontefract
WF8 2DD

What we need to know

Your first and second name, Your email address and What information you are looking for.

Please make sure you provide us with your name and address (or email) so that we get back to you as quickly as possible.

Possible charges

Charges may be made for actual disbursements incurred such as:

- Photocopying
- postage and packaging
- the costs directly incurred as a result of viewing information

If a charge is to be made, confirmation of the payment due will be given before the information is provided.

Payment may be requested prior to provision of the information.

Frequently requested information

Before submitting a Freedom of Information request, please check whether the information you are looking for is already available on our website.

Obligations under disability and discrimination legislation and any other legislation to provide information in other forms and formats will be adhered to when providing information in accordance with this scheme.

Appendix 3

High Well School Privacy Notice

Privacy Notice (How High Well School uses pupil information)

As High Well School is a maintained School of Wakefield Council, Wakefield Council is the Data Controller for the use of personal data at High Well School. This means that they are in charge of your personal information.

The categories of pupil information that we process include:

- personal identifiers and contacts (such as name, unique pupil number, contact details and address)
- characteristics (such as ethnicity, language, and free school meal eligibility)
- safeguarding information (such as court orders and professional involvement)
- special educational needs (including the needs and ranking)
- medical and administration (such as doctors information, child health, dental health, allergies, medication and dietary requirements)
- attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- assessment and attainment (such as any relevant results)
- behavioural information (such as exclusions and any relevant alternative provision put in place)
- trips and activities (such as personal identifiers)
- free school meals (identity management / authentication)

Why we collect and use pupil information

The personal data collected is essential, for High Well School to fulfil their official functions and meet legal requirements. We collect and use pupil information, for the following purposes:

a) to support pupil learning

b) to monitor and report on pupil attainment progress

c) to provide appropriate pastoral care

d) to assess the quality of our services

e) to keep pupils safe

f) to meet the statutory duties placed upon us by the Department for Education

The GDPR is part of the fundamental right to privacy and the law applies to any 'processing of personal data'. The UK data protection regime is set out in the DPA 2018 and the GDPR (which also forms part of UK law) Guide to the GDPR.

Processing shall be lawful only if and to the extent that at least one of the following applies:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Collecting pupil information

We collect pupil information via registration forms at the start of the school year and / or Common Transfer File (CTF) or secure file transfer from previous school

Pupil data is essential for the schools' operational use. Whilst the majority of pupil information you provide to us is mandatory, some of it requested on a voluntary basis. In order to comply with the data protection legislation, we will inform you at the point of collection, whether you are required to provide certain pupil information to us or if you have a choice in this and we will tell you what you need to do if you do not want to share this information with us.

Storing pupil data

We hold pupil data securely until the pupil reaches the age of 25 or 75 years if the pupil is on the Child Protection Register or a Looked After Child.

Who we share pupil information with

We routinely share pupil information with:

- schools / colleges
- local authorities
- youth support services (pupils aged 13+)
- the Department for Education (DfE)
- CAMHS (Child and Adolescent Mental Health Service)
- Social Services
- School Nurses
- IT
- West Yorkshire Police
- Youth Support Services / Careers Advice

Why we regularly share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

All information is transferred securely via Cryptshare or through the DfE Schools to Schools Service via Common Transfer File.

We share pupil data so that the appropriate support, guidance and advice can be tailored to pupils.

Department for Education

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our pupils with the Department for Education (DfE) either directly or via our local authority for the purpose of those data collections, under:

Section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

All data is transferred securely and held by DfE under a combination of software and hardware controls, which meet the current government security policy framework.
For more information, please see 'How Government uses your data' section.

Requesting access to your personal data

Under GDPR, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact:

Headteacher
High Well School
Rookwell Road
Pontefract
WF8 2DD

Depending on the lawful basis above, you may also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to seek redress, either through the ICO, or through the courts

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

For further information on how to request access to personal information held centrally by DfE, please see the 'How Government uses your data' section of this notice.

Last updated

We may need to update this privacy notice periodically so we recommend that you revisit this information from time to time. This version was last updated in November 2020.

Contact

If you would like to discuss anything in this privacy notice, please contact:

Business Manager
High Well School
Rookwell Road
Pontefract
WF8 2DD

How Government uses your data

The pupil data that we lawfully share with the DfE through data collections:

- underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school.
- informs 'short term' education policy monitoring and school accountability and intervention (for example, school GCSE results or Pupil Progress measures).
- supports 'longer term' research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school)

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools

The National Pupil Database (NPD)

Much of the data about pupils in England goes on to be held in the National Pupil Database (NPD).

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the department.

It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information

Sharing by the Department

The law allows the Department to share pupils' personal data with certain third parties, including:

- schools
- local authorities
- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

For more information about the Department's NPD data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

Organisations fighting or identifying crime may use their legal powers to contact DfE to request access to individual level information relevant to detecting that crime. Whilst numbers fluctuate slightly over time, DfE typically supplies data on around 600 pupils per year to the Home Office and roughly 1 per year to the Police.

For information about which organisations the Department has provided pupil information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police please visit the following website: https://www.gov.uk/government/publications/dfe-external-data-shares

How to find out what personal information DfE hold about you

Under the terms of the Data Protection Act 2018, you are entitled to ask the Department:

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the Department, you should make a 'subject access request'. Further information on how to do this can be found within the Department's personal information charter that is published at the address below:

https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter

To contact DfE: https://www.gov.uk/contact-dfe

Appendix 4

COVID-19 ADDENDUM

High Well School Appropriate Policy Document (Special Category)

During the COVID-19 Pandemic: Staff Test and Trace, Temperature checks (with or without recording), Informing PHE/DFE of test results, supporting NHS COVID-19 App, Health Professional data sharing.

This condition may for example apply where the processing is necessary for:

- public health monitoring and statistics;
- NHS resource planning;
- public vaccination programmes;
- responding to new threats to public health (eg epidemics, pandemics or new research findings);
- clinical trials of drugs or medical devices;
- regulatory approval of drugs or medical devices; or
- reviewing standards of clinical practice.

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require you to have an APD in place. (See Schedule 1 paragraphs 1(1)(b) and 5).

This document should demonstrate that the processing of SC and CO data based on these specific Schedule 1 conditions is compliant with the requirements of the General Data Protection Regulation (GDPR) Article 5 principles. In particular, it should outline your retention policies with respect to this data. (See Schedule 1 Part 4).

If you process SC or CO data for a number of different purposes you do not need a separate policy document for each condition or processing activity – one document can cover them all. You may reference policies and procedures which are relevant to all the identified processing. Whilst you may explain your compliance with the principles in general terms, without specific reference to each individual Schedule 1 condition you have listed, you should provide the data subject with sufficient information to understand how you are processing their SC or CO data and how long you will retain it for.

However if you rely on one of these conditions, your general record of processing activities under GDPR Article 30 must include:

(a) the condition which is relied upon;
(b) how the processing satisfies Article 6 of the GDPR (lawfulness of processing); and
(c) whether the personal data is retained and erased in accordance with the retention policies outlined in this APD, and if not, the reasons why these policies have not been followed.

The APD therefore complements your general record of processing under Article 30 of the GDPR and provides SC and CO data with further protection and accountability. See Schedule 1 Part 4 paragraph 41.

You must keep the APD under review and will need to retain it until six months after the date you stop the relevant processing. If the Commissioner asks to see it, you must provide it free of charge. See Schedule 1 Part 4 paragraph 40.

You should read this document alongside our Guide to the GDPR.

Note your APD does not have to be structured in accordance with this document. This template is intended as a guideline only.

Description of data processed

Give a brief description of each category of SC/CO data processed. You may wish to refer to your Article 30 record of processing for that particular data:

COVID-19 test results (Supporting NHS COVID-19 App, Test and Trace)
Temperature checks (with or without recording)
Supplying information to PHE and DFE
Data concerning health
COVID-19 Visitor Agreement information

Schedule 1 condition for processing

Give the name and paragraph number of your relevant Schedule 1 condition(s) for processing. Alternatively, you may wish to provide a link to your privacy policy, your record of processing or any other relevant documentation:

Duty of Care to staff and pupils
We have an information security policy (or equivalent) and take steps to make sure the policy is implemented.

Procedures for ensuring compliance with the principles

You need to explain, in brief and with reference to the conditions relied upon, how your procedures ensure your compliance with the principles below.

This helps you meet your accountability obligations. You have a responsibility to demonstrate that your policies and procedures ensure your compliance with the wider requirements of the GDPR and in particular the principles. The sensitivity of SC and CO data means the technical and organisational measures you have in place to protect such data are crucially important.

The questions listed in each box are intended to help you describe how you satisfy each principle generally, and are based on the checklist for each principle provided in the Guide to the GDPR. They are not exhaustive and are only intended to act as a guideline.

In explaining your compliance with the principles you should consider the specifics of your processing with respect to the SC and CO data you have identified above.
You may also wish to answer other questions which are included in our Guide to the GDPR checklists (see links in each section below).

There is also no requirement to reproduce information which is recorded elsewhere – **questions may be answered with a link or reference to other documentation, to your policies and procedures, Data Protection Impact Assessments (DPIAs) or to your privacy notices.**

Accountability principle
i. Do we maintain appropriate documentation of our processing activities? ii. Do we have appropriate data protection policies? iii. Do we carry out data protection impact assessments (DPIA) for uses of personal data that are likely to result in high risk to individuals' interests? See general checklist for Accountability and Governance.
Principle (a): lawfulness, fairness and transparency
i. Have we identified an appropriate lawful basis for processing and a further Schedule 1 condition for processing SC/CO data? ii. Do we make appropriate privacy information available with respect to the SC/CO data? iii. Are we open and honest when we collect the SC/CO data and do we ensure we do not deceive or mislead people about its use? See general checklist for Lawfulness, fairness and transparency.
Principle (b): purpose limitation
i. Have we clearly identified our purpose(s) for processing the SC/CO data? ii. Have we included appropriate details of these purposes in our privacy information for individuals? iii. If we plan to use personal data for a new purpose (other than a legal obligation or function set out in law), do we check that this is compatible with our original purpose or get specific consent for the new purpose? See general checklist for purpose limitation.
Principle (c): data minimisation
i. Are we satisfied that we only collect SC/CO personal data we actually need for our specified purposes? ii. Are we satisfied that we have sufficient SC/CO data to properly fulfil those purposes? iii. Do we periodically review this particular SC/CO data, and delete anything we don't need? See general checklist for Data minimisation.

Principle (d): accuracy
i. Do we have appropriate processes in place to check the accuracy of the SC/CO data we collect, and do we record the source of that data? ii. Do we have a process in place to identify when we need to keep the SC/CO data updated to properly fulfil our purpose, and do we update it as necessary? iii. Do we have a policy or set of procedures which outline how we keep records of mistakes and opinions, how we deal with challenges to the accuracy of data and how we ensure compliance with the individual's right to rectification? See general checklist for Accuracy.
Principle (e): storage limitation
i. Do we carefully consider how long we keep the SC/CO data and can we justify this amount of time? ii. Do we regularly review our information and erase or anonymise this SC/CO data when we no longer need it? iii. Have we clearly identified any SC/CO data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes? See general checklist for Storage limitation.
Principle (f): integrity and confidentiality (security)
i. Have we analysed the risks presented by our processing and used this to assess the appropriate level of security we need for this data? ii. Do we have an information security policy (or equivalent) regarding this SC/CO data and do we take steps to make sure the policy is implemented? Is it regularly reviewed? iii. Have we put other technical measures or controls in place because of the circumstances and the type of SC/CO data we are processing? See general checklist for Security.

Retention and erasure policies

You need to explain your retention and erasure policies with respect to each category of SC/CO data (this could include a link to your retention policy if you have one). You need to explicitly indicate how long you are likely to retain each specific category of SC/CO data.

Any information stored will only be used for the purpose it is intended for and will be destroyed when appropriate (i.e. Pandemic lowered to epidemic or threat eradicated).

APD review date
September 2021